CYBER INSECURITY

After 9/11, Kim Taipale changed his life. He started a think tank to study the future of war, specifically focused on global cyber threats. Now he advises Congress, CEOs and policy makers worldwide on the risks we all face.

Jay McInerney, left, and Kim Taipale chat in McInerney's sun-drenched penthouse about the threat of cyber-attacks.

photographed by JOSH LEHRER

Introduction by JANET ALLON

Like a lot of New Yorkers, Kim Taipale was profoundly affected by the events of 9/11. He and his wife, designer Nicole Miller, live within a half-dozen blocks of the World Trade Center and watched as the tragedy unfolded. That day and its aftermath played a major role in Taipale's decision to shift the focus of his career from investment banking and technology entrepreneurship to forming a think-tank. His Center for Advanced Studies in Science and Technology Policy is a nonpartisan research and advisory group that consults with both CEOs and government policymakers on how to deal with cyber crime, cyber terrorism, and, more generally, how to rethink questions of national security in a globalized world.

Taipale's interests and knowledge of cutting-edge technology make him one of the more fascinating—if perhaps disturbing—dinner partners you could ask for in the city. "I've known Kim for at least 20 years and I admire his inability to make small talk," says his friend, author and fellow downtown denizen Jay McInerney. "He inevitably raises the level of discourse at Manhattan cocktail and dinner parties." The longtime friends recently chatted about the Georgian cyber war, the perils of information technology and how your computer might be engaged in a cyber war without you knowing it.

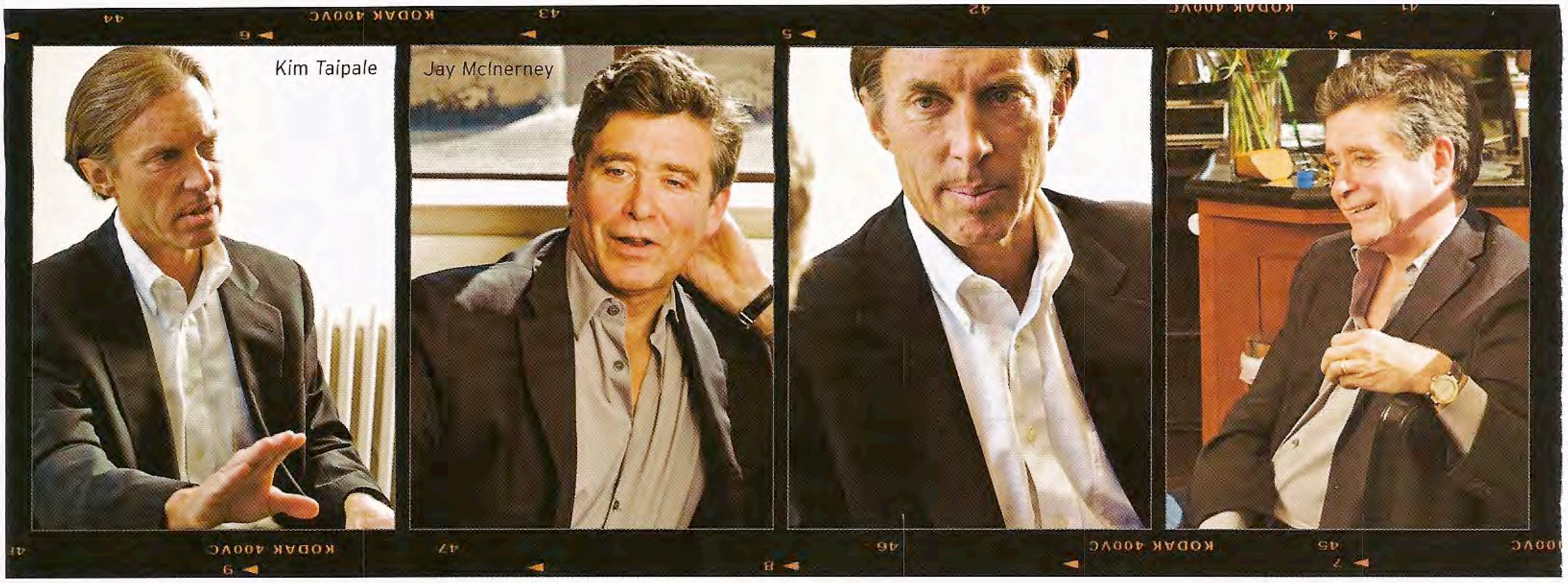
JAY MCINERNEY: What are the three major concerns of our government in terms of national security and cyberspace?

KIM TAIPALE: Clearly, the biggest national security threat is someone or some group getting a nuclear weapon and using it in New York, or Washington, or some other city. It's probably a lower probability risk than some other threats, but it's not like people aren't working on trying to make it happen. Terrorists may be living in caves, but it's not like they're not smart, motivated guys. It's a real threat.

Second is the emerging biotechnology threat. We are barely addressing how we would deal with the natural biological threats—SARS, the bird flu—what if Ebola got over here? We really don't have the mechanisms yet or have thought about how we would deal with an intentional attack, even though we have been through the anthrax episode. But the risk is increasing. We're moving to another level of biotechnology where people are learning how to create very serious pathogens. The DNA for the Spanish flu bug has been sequenced, and that sequence is available widely on the Internet. Being able to reverse-engineer DNA sequences back to the organism is something that certainly our kids will be able to do in a biology lab at some point.

These are esoteric but real existential threats.

On the cyber level, rather than focus on a specific threat, you need to think about the kinds of systemic vulnerabilities we have created as a society. This is the other side, the negative side of the cyber and information society. At the same time that we have empowered people and groups to do amazing things, create new businesses and opportunities, we've also created an increasingly fragile system for ourselves. A good example of this is the financial crisis going on right now. There have always been booms and busts and financial crises, but the ability for a financial crisis to start in a sub-prime market somewhere in the United States and then cascade through all of these other markets would not have been possible without the interconnection



and interdependency of all these other markets. In large part these interdependencies were enabled by information technology.

You have to think about "cyber" in the sense that information technology is the control device for a lot of other things. It's like the global nervous system. The threat lies in attacking computers and computer systems as control devices for real things: financial markets, chemical plants, utilities. These attacks that can result in cascading failures across society are much greater threats than simply attacks on computers themselves.

The problem for everybody, but particularly for the U.S. government, is how do you protect something where 90 percent of the infrastructure is in private hands?

JM: How vulnerable is the national security of our country to cyber-attack? In the recent war between Russia and Georgia, it seems that there was a concerted effort to tie up the Georgian security computer systems, but it wasn't clear what the impact was. Are we vulnerable to that kind of attack?

KT: An interesting way to look at that is to compare the Georgian experience to the Estonian experience. Estonia was subject to the same kinds of cyber-attacks in April 2007, in connection with its own political conflict with the Russians. They came under heavy cyber-attacks for about three weeks, which essentially shut down the country, the banking system and government services. At the same time they are a very small country, so they had very few connections and limited bandwidth to the outside world. They were essentially "cyber landlocked."

You have to understand that these kinds of cyber-attacks are not really the hacking kinds of attacks, where someone breaks into the system and makes it crash. These are distributed denial-of-service attacks where the attackers get many computers to send commands to a server at the same time and it gets overwhelmed. It's more like a traffic jam. Today, the tech administrators of large U.S. companies manage those kinds of attacks every day.

> "The DNA for the Spanish flu bug has been sequenced and that sequence is available widely on the Internet."

Georgia wasn't as dependent on the Internet as Estonia, so it didn't really bring things to a halt there. But it did bring down the Web site of the parliament and the public Web sites of the defense department, the foreign ministry and others. That prevented the Georgian authorities from using these servers to put out information to their own population and to the world.

These attacks are interesting because they are launched by just a few people who essentially control large farms of computers. In fact, your computer may have been involved in that attack.

JM: How does that happen? That idea has scared me ever since I became aware of it, that my computer, at night, might be performing all sorts of nefarious activities.

KT: It's very likely that it does.

JM: It's like finding out that you have a tapeworm.

KT: Or worse: A tape worm that can go out and attack your neighbor while you are sleeping.

JM: But how does that happen?

KT: Your computer can be compromised in many ways. It used to be that you could basically protect yourself if you didn't run software that you hadn't bought yourself, or didn't click on any attachment that came in e-mail from unknown sources. But, things have evolved away from the e-mail attacks to where most attacks occur through compromised Web sites. You just go to a compromised Web site and it downloads malicious software onto your computer.

> "Of the top hundred Web sites in the world, legitimate sites like Facebook and MySpace, 60 percent of them had malicious software on them at some point."

JM: I was just thinking it would be kind of clever and effective to compromise porn Web sites, for instance—you know, heavily-trafficked Web sites.

KT: Google did a study of the top hundred Web sites in the world, legitimate sites like Facebook, MySpace, etc. Sixty percent of them had malicious software on them at some point.

JM: But there seems to be some sort of line that was crossed in the case of Georgia, when a governmental entity orchestrated a guerrilla cyber-attack. Traditionally, it's been individuals, or lone gunmen or groups of them hacking, or conducting scams. It seems in the case of Estonia and Georgia that the Russian government was either orchestrating or strongly encouraging the cyber-attack.

KT: Well, that is the interesting question. Was the Russian government behind the attacks? Were they orchestrating it, or encouraging it? The real question is: Is it worse for national security or global stability to find out that it was the Russian government that did it or that it was just an unorganized mob of hackers? If it's just an unorganized gang of hackers, that means that every time you have an international crisis in the future, hackers can join in from their bedrooms and escalate it. During the Georgian incident, hacker Web sites in Russia published software tools that made it possible for anyone to join the battle against Georgia. A Salon writer actually did this, joined the cyber militia. That seems to me more dangerous to stability, at least in the near term, until we figure out how to deal with it. If it's the Russian government, you can use the regular levers of power. If it is just a bunch of hackers, then it means governments are losing some of their control to manage international crises.

A lot of these attacks seemed to have originated with one or two people. They post on the blogs what they are doing, and other people join in. At some point, it gets to a tipping point. Then, all of a sudden you see botnets starting to join in. Botnets are controlled through servers by criminal organizations that have built these up to use for scams over time. A lot of those botnets, which are large networks of compromised computers, are available to anyone for hire. There are literally hacker Web sites out there where you can go online and hire one of these botnets for any purpose—to send spam, or to launch a denial-of-service attack.

The most notorious example of this kind of organization is the Russian Business Network in St. Petersburg, which is essentially a criminal Internet service provider.

They set up a system just like a legitimate ISP [Internet Service Provider], like the one that provides you with service at home—only their services are aimed at people with criminal intent.

With these attacks in Georgia and Estonia, when the botnets joined in the attack, they were traced back to command and control servers known to belong to the Russian Business Network. That's part of the circumstantial evidence that people use to say that the Russian government was behind these attacks.

There is the feeling that the Russian government could close them down if they wanted to. But by passively allowing this activity to go on, they have enabled this to happen because it serves the government's interests. Plus, of course, there are rumors that the people involved in starting the RBN are ex-KGB.

The Chinese and the Russians in particular seem to tolerate this sort of behavior—these cyber-crime gangs—as long as these groups hack outside their own country, and by allowing them to exist, they are keeping in their quiver, if you will, resources that they can use.

> "With these attacks in Georgia and Estonia, when the botnets joined in the attack, they were traced back to command and control servers of the Russian Business Network."

The Chinese have a very active program right now against the U.S. on the economic espionage front.

JM: What are the Chinese after?

KT: Everything. Biotechnology, drugs, technical designs for airplanes, weapons systems, pure economic espionage.

This has been going on forever, only now, we are in a new world where chips and software make it really easy to hide things or steal things.

A lot of malicious software, criminal software that steals your passwords and such, is coming in through hardware devices.

A significant part of this kind of activity is more criminal than Chinese government activity. But, there are more than 120 nation states with active cyber-espionage programs. We're doing it to the Russians and Chinese. They are doing it to us. And all the other countries, including our allies, are doing it to everyone, as well.

JM: In terms of the sub-state entities, is a group like Al Qaeda sophisticated in these areas? We know they are sophisticated in using the Internet to spread their message, and communicating among disparate cells and so on, but are they sophisticated on the level of hacking, sabotage or espionage?

KT: A cyber-attack is generally not the kind of thing terrorists are interested in. It's not spectacular enough, it doesn't make for compelling TV news coverage. But there is the connection between terrorist groups and cyber criminals. There, you see a sophisticated effort. For a number of terrorists, particularly in Indonesia, part of their efforts have been to put out manuals and instructional materials to tell people how to do cyber crime and cyber fraud to fund terrorist activity.

> "Defense is always going to lag behind offense. You may not even know about all your vulnerabilities, and you're never going to know about all of the people who are trying to attack you."

JM: Do we have any leverage? For example, how do we get the Russians to become part of the solution?

KT: It's not going to be easy. We have to change how we think about security. We have to become smarter and a little more nuanced about how we do things. In the old world, when nation states were what you had, whoever had the most tanks won. It's getting more complicated in an interdependent world and where non-state actors are players. You can't use force the way you used to. Every time a country like the U.S. uses force, even if we kill just one or two people, the blowback, the bad press from doing that, really constrains a country like us from using that kind of hard power. For terrorists, to use violence is a success strategically, even if it's tactically insignificant. For counterterrorism, particularly for the U.S. or other major powers, the use of violence is actually a strategic failure even if it is tactically successful, even if you wipe out the terrorists—because you've already admitted, by using violence, that all of your normal systems, all of your laws, all of your regular civilized behavior, have failed. The asymmetry is in the very perception of how you use power.

JM: Is cyber security keeping pace with the people who are trying to attack us?

KT: I would say no. One of the problems with cyber, and perhaps biotechnology, too, is that defense is always going to lag behind offense. You may not even know about all your vulnerabilities, and you're never going to know about all of the people who are trying to attack you and all of the ways they can attack you. It's the same problem with real security. You're never going to be able to be certain. You have to assume that there is an open back door somewhere. You try to minimize the consequences of an attack, and you try to be resilient so that you can recover. ✦