BGS Senior Counselor Michael Morell Discusses Cybersecurity Threats And Potential Solutions To Disagreements Between Government And Tech Companies Regarding The Use Of Encryption

Cyber Threats: Only Getting Worse

The Cipher Brief | April 20, 2016
By Michael Morell

It seems like the cyber domain has recently been awash in controversy. From major hacks that compromise the information of millions of people, to bitter legal disputes between tech giants and law enforcement, to a steadily expanding number of threats, cybersecurity has never seemed so crucial. Former CIA Acting Director and Deputy Director Michael Morell spoke with The Cipher Brief about his assessment of the growing cyber-threat, as well as a potential solution to increasingly contentious discord between government and the tech industry on the topic of encryption. For the former, he recommends specific types of tools that you monitor anomalous activity on your network and for the latter, a comprehensive push by the intelligence community to find a way to access encrypted information without compromising American companies.

The Cipher Brief: How do you see the cyber threat, and how is it evolving?

MM: In order to think about the threat in the most useful way, it is important to think about the adversaries. When you do that, a couple of things jump out. First, the threat is going to get worse. The number of

nation states with the ability to conduct cyber operations is expanding, because the tools one needs to get inside a network, to steal data, and to do damage are increasingly available on the black market, largely in the deep web. So, smaller countries, which don't have the resources to develop their own capabilities, can now simply go out and buy them. At the same time, the number of cyber criminals is growing at an alarming rate, because there is so much money to be made from cyber crime (such crime now generates more revenue than the illegal drug trade). And, terrorist groups, which have not been focused on cyber attacks, now are becoming more interested.

Second, while the different types of adversaries are numerous (nation states, organized crime groups, terrorists), perhaps the most dangerous potential cyber adversary comes from a group that most people do not think about – your own employees. Whether recruited by an outside group to conduct cyber operations against you or whether taking some cyber action on their own because they are angry with you for some reason, your employees represent the greatest threat to your network. While the vast majority of your employees will, of course, never become a threat, it only takes one to do enormous damage – Snowden being the best example. When it comes to cyber defense, most companies are focused on protecting their network from outsiders. They need to be just as focused on insiders.

TCB: What about defense?

MM: A few thoughts. First, there is a taxonomy of cyber defense that makes sense to me – rigorously assess the vulnerabilities you face (from both outsiders and insiders) in relation to what you need to protect, put in place the tools and the policies you need to mitigate those vulnerabilities, and purchase cyber insurance (an emerging industry) as the ultimate guarantor against potential financial losses.

Second, the most important tools are the ones that allow you to quickly identify when someone is in your network, to be able to see what they have done, and to get them out. Such tools are important because there is no way to keep out all adversaries – a sophisticated and persistent

adversary will always find a way to get in – and because speed in identifying the intrusion is essential to minimizing the damage. Most companies are using behavioral algorithms to identify intrusions – similar to what credit card companies use to detect potential fraud. But I do not believe these tools are the best ones, as they produce too many false positives and because the adversary can and will discover the algorithms and therefore avoid creating a red flag. No, in my view, the much better approach is the emerging tool of deception – deceiving the adversary in a variety of ways to include deceiving them into telling you that they are in your network.

Third, in terms of keeping people out of your network in the first place, there are obviously a lot of tools available to do that, but there is nothing more important than educating your employees on what to do and what not to do with the emails and the attachments to emails that they receive. Phishing attacks are, by far, the most common method that adversaries use to get into a network. Unaware and non-disciplined employees unwittingly enable the vast majority of sophisticated attacks.

Fourth, cyber security is always going to be a moving target. The adversaries will always get better; they will always adapt to the defense of the day. So, the defense has to adapt as well. There is no defense that is permanent. And the best defense is always going to come from those firms who themselves think like the bad guys – essentially asking themselves, "how would I get what I want from that network and therefore how would I defend against it."

TCB: What does the government need to do?

MM: I'm concerned that this piece of the puzzle is furthest behind. Yes, we finally got some good legislation that provides liability protection for firms sharing information with the government. But, the government has a long way to go to figure out its role in defending private industry against cyber attacks. Here are some ideas that I believe are worth thinking about.

One, the stealing of intellectual property for the purposes of advancing the economic interests of specific industries and firms should be treated by the World Trade Organization as an unfair trade practice. A penalty should be imposed on those industries that take advantage of stolen intellectual property. Simply indicting people for the theft has little deterrence effect for those hackers who work for foreign governments and who have no plans of, or interest in, ever traveling to a place where the indictment could actually be enforced.

Two, the UN should take on the responsibility for establishing norms for cyber warfare. And, of course, before that can happen, the U.S. needs to sort its own views on what these norms should be. What might they be? Perhaps attacks on critical infrastructure directly associated with a country's military are fair game; perhaps attacks on all other critical infrastructure are not. Even if all nations can't agree on a set of norms, we can be clear about what is acceptable and not acceptable to us and to our closest allies, and what the costs would be if others violate them.

Third, there should be an international organization formed to tackle cyber crime – an organization where the information on cyber crimes comes together and can be packaged in a way that local authorities can act on them.

Fourth, those countries that refuse to abide by international norms on cyber warfare and that refuse to either put tough laws on the books against cyber crime or refuse to enforce those laws should face tough sanctions, the same kind of tough sanctions that forced Iran to the negotiating table on the nuclear issue. Again, simply indicting people 10 thousand miles away has little deterrence affect.

Fifth, the United States needs to come to a policy decision on the use of cyber offense for defensive purposes. That is, if all the above fails, we need to decide if we are going to use our considerable capabilities to stop a cyber attack on a U.S. entity that the government sees coming. Preemptively. There are lots of tough issues here, but at the end of the day, the government has a Constitutional responsibility to

protect Americans, including against cyber attacks.

TCB: Is it really possible to do all these things?

MM: Absolutely. We just need to work through it step by step, both at home and abroad. I think the Cyber Commission that President Barack Obama just established is a very important step.

TCB: What is your reaction to the continuing controversy between the FBI and Apple?

MM: I have four thoughts. The first is that both sides in the debate have a very compelling argument. The FBI's powerful argument is how can you (Apple) not help us discover if there is information on a phone that might save lives? Apple's powerful argument is how could you (the government) ask us to do something to our operating system that would create a broad security vulnerability that any number of adversaries would most definitely exploit and that would severely damage a U.S. industry that is so important to the future of the economy?

Second, where I come out on all of this, and here I am moving from the narrow issue of getting into a specific phone to the broader issue of keyless encryption, is the result of a simple practical consideration—that the vast majority of the communication applications that are encrypted without keys are outside the U.S. There are literally hundreds of them. If the government forces U.S. firms to create keys for their encryption, the bad guys would simply communicate using keyless apps produced overseas. In that highly likely scenario, there would be little gained in terms of security, but there would be a significant loss to U.S. firms (their apps would be less secure and fewer people would use them as a result).

Third, I can't remember a time during my service in government when we physically had an IT device in our hands and we could not ourselves get the data from it that we needed. The fact that multiple U.S. agencies could not get into the phone of the San Bernardino attacker was, for me,

a wake up call that advances in technology had outstripped the capabilities of the U.S. Government. We should see it as a Sputnik moment.

And this sets up the fourth reaction, that the conversation on this very important issue is not occurring in the right place. What do I mean by that? The conversation now is taking place between the government and industry. Before the FBI found its way into the phone of the San Bernardino attacker, based on a suggestion from an outsider, the conversation was taking place between the two in the courts and in the media. And that conversation continues with regard to other specific phones and with regard to the broader issue of keyless encryption.

TCB: If the conversation should not be between the government and the private sector, where should it be?

MM: It should be occurring within the government. What does that mean? In my view, the National Security Advisor should say the following to the Director of National Intelligence, the Director of CIA, the Director of the FBI, and the Director of NSA: "The President's expectation is that we, that is you, should have the capability to break the commercial, keyless encryption being used by our adversaries, and that we should have the ability to get inside a particular IT device that is in our possession. We should keep our ability to do these things one of our most closely guarded secrets. And, if we need a Manhattan Project style effort to get us there, the President will support that. Get to work."

Achieving this vision would give us the best outcome. We would have the ability to read the communications of the bad guys, they would not know it, we would not be asking any U.S. companies to weaken the security of their products, and we would not be undermining them in the market place.