The Attribution Revolution:
Raising the Costs for Hackers and Their Customers

Statement of Stewart A. Baker

Partner, Steptoe & Johnson LLP

Before the Judiciary Committee's Subcommittee on Crime and Terrorism
United States Senate

May 8, 2013

Mr. Chairman, Ranking Member Graham, members of the subcommittee, it is an honor to testify before you on such a vitally important topic. I have been concerned with cybersecurity for two decades, both in my private practice and in my public service career, as general counsel to the National Security Agency and to the Robb-Silberman commission that assessed U.S. intelligence capabilities on weapons of mass destruction, and, more recently, as assistant secretary for policy at the Department of Homeland Security. In those two decades, hacking of computer networks has evolved from occasionally annoying pranks into a full-fledged counterintelligence crisis.

Today, network insecurity is not just an intelligence or law enforcement concern. It could easily cause the United States to lose its next serious military confrontation.

I have been broadly supportive of recent efforts to improve the security of our networks, and I still am. But let's not kid ourselves. Today, even our most secure systems are being compromised. Security professionals don't expect to keep hackers out of their networks; all they can hope to do is – perhaps – isolate and protect some really sensitive data. And, to tell the truth, after multiple demonstrations that hackers can reach completely isolated networks, no one is offering any guarantees that they can do that, either.

Our network security, in short, is toast. We've been living in a dream world, thinking that if we could just fix all the security holes that hackers have been exploiting, then our networks would at last be secure. But if that dream were ever achievable, it looks hopeless today. The resources that hackers are putting into finding holes are growing steadily, as the modest risks and great rewards of exploiting networks continues to attract everyone from nation states to organized crime.

In short, we can't defend our way out of this fix, any more than we could solve the problem of street crime by firing our police and making pedestrians buy better body armor every year.

The ineffectiveness of our current strategy is clear. As it is, the great majority of companies that get hacked only discover the intrusion when they are told by a third party, like the FBI. And by the time companies learn of the intrusion, on average, the bad guys have been in their computers for months if not years. We need to find another paradigm for improving our security.

Attribution 101

That is why I will focus my remarks today on what is shaping up to be an "attribution revolution." The theory is simple. The same human flaws that have left our networks ever more exposed to attack are undermining our attackers' anonymity. This is what I like to call Baker's Law: "Our security may be toast. But so is theirs."

As numerous recent reports show, attackers are only human. They make mistakes when they're in a hurry or overconfident. They leave bits of code behind on abandoned command-and-control computers. They reuse passwords and email addresses and computers. Their remote access tools are full of vulnerabilities. These are openings that private researchers – from Mandiant and Trend Micro to SecDev and the Citizen Lab – have exploited; they've traced cyberattacks to the command and control computers used to carry them out, then to homes and offices of the hackers that perpetrate them. These reports have identified individuals and institutions closely associated with hacking US companies and agencies. They've found the universities where the hackers trained. They've found the hackers' names and instant message addresses . Using these clues, researchers have even tracked the hackers down and called them up for comment. They've found the companies that employ the hackers today. In at least one case, hacking victims in the Republic of Georgia have turned the tables and used their attackers' malware to take an attacker's picture with his own desktop camera.

The attribution revolution has truly begun.

From Attribution to Deterrence

But attribution is only half of the formula if we want to deter cyberespionage. The other half is retribution. Once we identify our attackers, we need to persuade them to choose another line of work.

That does not necessarily mean that we should rely exclusively or even primarily on the Department of Justice or the Federal Bureau of Investigation. We must look beyond traditional criminal prosecutions to deter cyberespionage. Once we do, we will find plenty of tools at our disposal:

1. Expose and Isolate Nations

Naming and shaming is a commonly used method of deterring bad conduct by other nations. The U.S. may be reticent about releasing hard-won intelligence about the activities of foreign governments. But some of the most explosive – and convincing – recent allegations against foreign governments have in fact been made by private entities. The report released earlier this year by Mandiant offered extensive evidence of the People's Liberation Army's role in hacking into U.S. companies over a number of years. The report placed an embarrassing spotlight on state sponsored hacking in China and sparked bitter but vague denials from the Chinese government.

Of course, it's not clear that embarrassment alone will stop countries like China or Iran or North Korea from supporting cyberattacks against our companies and our government. But it's a start. It raises the cost of what has been a relatively low-risk, asymmetric strategy. It strips them of a sense that they are protected by a veil of ambiguity about the origin of attacks on our networks. And it sets the stage for further action in the future.

2. Sanctions for Spies – And Their Enablers

The Justice Department and the FBI may not be able to reach hackers located on the other side of the world. And even if we could catch them, we might not want to risk compromising intelligence sources and methods by taking them to court. But that does not mean we cannot punish them. We already use classified information to identify terrorist supporters and drug kingpins as "specially designated nationals" and to impose sanctions on them – seizing their bank accounts and assets, for example, and prohibiting U.S. citizens from doing business with them. We even have such programs for sanctioning Belarusian kleptocrats and those who traffic in conflict diamonds. Maybe it makes sense for the American government to use sanctions to punish misdeeds in Belarus or West Africa, but it surely makes a lot more sense to use these measures to punish people who are invading homes and offices across the United States?

To tell the truth, I don't know why the President hasn't done this already. He's got all the authority he needs to impose sanctions on cyberspies and their enablers. Under the International Emergency Economic Powers Act, the President could determine that cyberspying poses "an unusual and extraordinary threat" to the United States and declare a "national emergency." He could then publish a list of hackers who would be subject to sanctions. In keeping with past practice, he could rely heavily on classified data to make the designations – without disclosing any of it.

3. Visas

One of the things that Mandiant disclosed was how much some of our adversaries hate their jobs. They found a blog maintained by one notorious hacker, and all he could talk about was his dream of making a "prison break" from his 9-to-5 job stealing secrets.

Maybe we should help him out. The Justice Department is authorized to issue a couple of hundred "S" visas each year to foreign nationals "in possession of critical reliable information concerning a criminal organization or enterprise." The visa allows family members to enter as well, and it becomes a permanent residency if the witness's "information has substantially contributed to the success of an authorized criminal investigation."

Systematically hacking US companies and agencies surely constitutes a criminal enterprise under US law, and I note that an investigation can apparently be deemed a success without leading to a criminal conviction. If a witness's cooperation helps us to thwart other countries' cyberspying campaigns, that surely counts as a success.

On the flip side, the U.S. government also has the power to deny visas and other perks to entities that act as enablers to hackers.

For example, late last year Trend Micro released a report that unmasked "Luckycat," a Chinese hacker who had attacked the Dalai Lama, aerospace firms, and other targets. His real name, according to the report, was Gu Kaiyuan, formerly a student at Sichuan University's Information Security Institute and at least at the time an employee at a major Chinese Internet company, Tencent.

Now we can't reach Mr. Gu in China, but why haven't the officials investigating those intrusions gone to his employer and his alma mater and asked them to cooperate in the investigation? Unlike Mr. Gu, these institutions benefit mightily from good relations with the United States government. Sooner or later, every Chinese university wants its students and faculty to get visas to work and study in the United States. And every Chinese company that does business here is subject to our investigative authority. They have many reasons to cooperate, particularly to rebut any evidence that they condoned or enabled cyberspying. At a minimum, taking a hard look at these institutions will make them think twice before they support or turn a blind eye to hackers in their midst.

4. Criminal and Civil Suits for Final Customers

But punishing individual hackers is only part of the story. What if we applied all of these measures not just to the hackers themselves but to companies that benefit from the data they filch from U.S. networks? There's not much difference in criminal responsibility between a thief and the guy he's stealing for. But there could be all the difference in the world between hackers who do their work from the safe environs of a protective government agency and the hackers' customers, who can't be truly successful in today's world if they aren't part of the global marketplace. And going global means exposing their companies, executives, and assets to the legal systems of the United States, Europe, and a host of other countries that are pretty much sick of wholesale espionage aimed at their companies. If a few big companies find that having a cozy relationship with their government's hackers means criminal prosecutions and asset seizures, they're a lot more likely to say "Thanks, but no thanks" to offers of stolen data.

Of course, to bring those cases, we'll have to have those companies dead to rights, and so far we don't. US security researchers have done a great job of tracking the thieves back home. But they've had trouble identifying the companies who ultimately benefit from cyberspying.

That too is an attribution problem – the next one we have to solve if we want to really discourage commercial cyberespionage. It will be difficult, but no harder than the first attribution problem looked five years ago. Nailing the customers for stolen data is going to take a major intelligence campaign, but in the end I think we can identify with certainty both the cyberspies and their spymasters.

What Role for Private Companies?

This brings me, finally, to the role that private companies should play. I'll be blunt. We can't rely exclusively on the Federal Bureau of Investigation. Sure, when combined with our intelligence assets, the FBI has resources and authorities that exceed those of any single

company. But in aggregate, it's the private sector that is spending the most to counter cyberspies. When the FBI discovers that a company has been compromised, it tells the victim, but it rarely offers technical advice about how to identify or thwart the attacker. Instead, the victim hires a company like Mandiant to deal with the attack. These private investigators know their adversary. They can often tell who the attackers are by the tools and tactics they use. They can often gain access to the command and control machine used for the exploit, where they find the clues that help them confirm their attribution of the attack. This is all information gathered by private investigators. To be frank, it is information that the FBI would never gather on its own. The Bureau doesn't have the manpower and it doesn't have the technical capacity to investigate all of these intrusions in such detail. And, given the current budget climate, it never will. Only in the private sector are we likely to see a continued rise in expenditures to fight network attacks and cyberespionage.

So, if we want to take full advantage of the attribution revolution, we can't simply leave this to the Bureau and the prosecutors. We need better ways to draw on the resources of the private sector and their investigators.

Right now, however, the Justice Department is doing more to hurt than to help companies that want to respond aggressively to the theft of their secrets and their intellectual property.

Let me give you one example. Suppose that a private investigator finds that data is being exfiltrated from his client to a particular command and control server. If the server is in the United States, the investigator may be able to persuade the owner, who is probably himself a hacking victim, to grant access to the server. This happens a lot, and it has great value, especially for attribution. The investigator may be able to identify the attackers and even recapture some of the stolen data.

But what if the hackers get wise and move the server to another location that they actually own? Can the investigator follow them to that other server and use what he knows about the gang's passwords to get access to the evidence and the stolen data stored there?

Not according the United States Department of Justice, which has begun actively and publicly discouraging any investigations that do not rely on the consent of the network owner, even when the network owner is the hacker himself. Recently, an anonymous Justice Department spokesman told Bloomberg BNA that intruding on an attacker's network would be both bad policy and "likely a violation" of the Computer Fraud and Abuse Act.

This is unfortunate in so many ways that I can understand why the spokesman insisted on anonymity.

Remember that the FBI is not itself gathering such information from foreign command and control servers – or doing much else to stop individual attacks. And, as we've seen, the FBI simply can't be expected to keep up with the current wave of attacks. Companies suffering massive cyberespionage losses are getting about as much attention as an Adams-Morgan resident whose bicycle has been stolen from the lamppost outside his home.

So when it says that private investigations into other networks are "likely a violation" of federal law, the Justice Department is really saying, "We may not be able to protect you from hackers, but we sure can stop you from protecting yourself."

This view has particularly hampered efforts to track attackers back to their headquarters. In many cases, private investigators know exactly where those headquarters are located and have a pretty good idea what passwords would get them into the network. But those networks are certainly owned by their attackers, and the prospect of being prosecuted means that only the bravest and most outraged victim is likely to take the risk of following his attackers home – and even if he did, it isn't clear what he could do with the evidence he gathered, since the Justice Department might decide he's easier to indict than the hacker

The problem is a lack of imagination–in particular, a belief that the only choices are wise, temperate, and ineffectual rule by government prosecutors on the one hand and a pitchfork-wielding mob of vigilantes on the other.

But in the real world, we have many more choices than that. If someone stops making payments on a car loan but keeps the car, the lender doesn't call the police. He hires a repo man. In the real world, if your child is kidnapped and the police aren't making the investigation enough of a priority, you hire a private investigator. And, if I remember correctly the westerns I watched growing up, if a gang robs the town bank and the sheriff finds himself outnumbered, he deputizes a posse of citizens to help him track the robbers down.

That's where we are now. Things a lot more valuable than a car have been stolen; the police aren't able to help; they barely have the resources to protect themselves; and they're definitely outnumbered.

Private investigators and deputized citizens and repo men aren't the same as vigilantes or a lynch mob. They are institutions that allow the victim of a crime to supplement law enforcement – while also providing social control and oversight of the victim's actions. The time has come to experiment with the same kind of institutions for cybercrime. The Justice Department and the Bureau should be required to let responsible private investigators work as adjuncts to government and to use carefully supervised portions of government authority as they gather evidence to identify hackers.

If we can do that much, we will go a long way toward gathering the attribution evidence we need to truly deter these attacks. This is not simply speculation. A recent cybersecurity report from two Luxembourg entities, a private computer incident response team and iTrust Consulting illustrates the potential for such an approach. The researchers that prepared this report, led by Paul Rascagnères, were able to break into and map the command and control infrastructure of a notorious Chinese hacking unit. In fact, he did to them what they have been doing to us – breaking in, logging the attackers' keystrokes and stealing their passwords, and then while they were searching for the intruder on their network, packing up their tools and stolen data and exfiltrating everything out from under their noses.

That kind of thing shouldn't be done without government oversight. And it cannot be done without the help of security professionals working for the victim. It's time to find a new way forward.

A Strategy For Exploiting the Attribution Revolution

Government agencies do many things well, but finding a new policy direction isn't usually one of them. This committee can play a valuable role in making clear that the government needs a new strategy for the cybersecurity crisis.

Some of the recommendations I made earlier could be incorporated into a new strategy. For example, Congress could adopt legislation imposing sanctions on foreign hackers and their customers. Congress has done this on numerous occasions to punish human rights violations abroad, as with the recent Magnitsky Act. Why not impose sanctions this time on those who have violated the human rights of Americans right here in the United States?

Similarly, Congress could supplement the "S" visa to make it more effective in combating cyberespionage. This could include increasing the number of "S" visas or allowing agencies other than the Justice Department to issue such visas. Congress could also authorize DHS and the State Department to deny visas to institutions that enable hacking activities.

Finally, Congress can do more to enable retribution against large companies that benefit from information stolen by hackers. At the outset, this should include providing sufficient authorities, resources, and encouragement to the Intelligence Community so it has the capacity to track down stolen data. Congress may also wish to consider laws that make it easier for victims to sue these companies, for example by encouraging them to piggyback on successful prosecutions.

Conclusion: Our Best Hope is a Change in Strategy

In closing, let me return to my main theme. We face a crisis. Cybersecurity is bad and getting worse. Civilian lives, our economic future, and our ability to win the next war, depend on solving our security problems. We need to find ways to turn the tables on hackers by putting the pressure on them and the entities that sponsor and enable them. To do this, we need to shift to a more active defense posture—one that relies on attribution and retribution.

In my view, this shift would be best achieved if we find ways to allow victims to use their own resources, under government oversight, to identify the people who are stealing their secrets and the institutions that are benefiting from the theft.

The first step in the shift is to acknowledge how bad things are, and how seriously our current institutions have failed. The next step is to chart a new course.

The good news is that we have taken the first step.

The next step is up to you.