黑客、泄密者及创新

■泰德·普林斯(Dr. E. Ted Prince)
佩斯领导力研究院创始人兼总裁

黑客

目前很清楚，美国多数大型企业和美国政府机构常常受到黑客“造访”。美国媒体称，其中相当一部分来自于中国，甚至还指出上海某栋楼就是中国黑客的一个源头。

假如我是中国的黑客，我也会侵入美国的电脑系统——谁知道美国到底在钓鱼岛问题上会做些什么？类似这些，中国当然想知道。

中国不是唯一的例子。比如，有数不清的美国金融机构不断报告称遭到了来自伊朗的黑客侵入。这个国家正是美国经济战打击的目标，因此它这么做并不稀奇。

我们不能认为，针对美国机构发起黑客举动的一定是美国的敌人。几乎可以肯定的是，美国的朋友也常常这样做，以色列就是一例。当然，也不能断定欧洲或是其它美国的盟友不会“黑”美国。即使大家都是盟友，它们也仍想知道美国正在做什么，并想让自己做好准备去应对一些无法公开讨论的可能性。

而且，我们知道，美国的黑客也在侵入其它国家，当然包括中国。我们甚至还知道，其中的一些攻击源具体来自美国的哪些大楼。美国对中国的黑客举动比中国对美国的多，这个可能性不是不存在。事实上，美国对中国的黑客攻击很有可能不仅规模巨大，而且十分复杂，有些或许甚至已经超出中国的认知。

作为证据，可以看看美国针对伊朗的黑客行动。我们知道，美国和以色列曾联手用高度复杂的数字病毒侵入了伊朗的工业和工业离心机，使伊朗的一些核浓缩项目受到严重破坏。这只是我们知道的。我们不知道的呢?恐怕还要多得多。

所以，毫无疑问，美国受到黑客攻击的同时也在发出攻击。

国防要面对的也因此不仅仅是战斗机和航母，其前沿应该是数字与黑客技术。

黑客的目标往往有两类，一类是军事，另一类则是商业。

就美国媒体的报道看，相当一部分中国黑客将目标对准了美国商业信息及技术机密。这可能是真的。

我设想，其它很多国家也在做着同样的事情。当你是世界一流的创新者时，每个人都想知道你的商业秘密。即使一些这样的活动是不合法或不道德的，但或许至少并非所有这类活动都是非法的。

而且我认为，一些国家通过黑客技术获取美国公司的商业机密甚至是存在一些社会和商业价值的。这会让它们更快地进步，它们的人民或许会因此变得更加富有，也能消费更多东西，包括来自美国的商品。因此，或许每个人都可以从侵入商业的黑客活动中有所得，尽管商业机密被盗的美国企业不这么认为。

但有一点值得注意：更多国家黑客针对的是美国的军事。虽然也有很多国家针对美国的商业组织，但相比之下较少。这是因为，在法治强大的国家，雇员如果知道他们的雇主在用黑客技术窃取其它国家的商业机密，是可以将他们告上法庭的。因此，多数发达国家不会对美国的商业秘密采取黑客举动，尽管仍有一些在高度保密下进行。

反过来，美国无疑也在频繁地通过黑客技术获取包括中国在内的其它国家的军事秘密，但可以肯定的是，美国的企业基本上不会去“黑”其它国家的商业秘密。因为在美国，同样有强大的法律鼓励雇员检举这种做法并在政府的帮助下将这样做的雇主告上法庭。因此，美国企业很少敢这样做，除非是非常小的私人企业。

因此，美国或许在军事领域的黑客行为比其它国家多，但在商业领域，应该相当少。

解密者

听说过“维基解密”(WikiLeaks)吗?这是一个由澳大利亚人朱利安·阿桑奇运营的网站，任务是将政府的一切秘密公之于众。它的理念是，公民只有在完全获知政府内部的通信时才算自由，包括军事机密。“维基解密”已经公布了数百万页美国军事秘密，目前仍致力于通过黑客技术挖掘更多。

> 黑客口水战
> 反映出的是
> 实施黑客行为的国家
> 在社会与经济上的
> 竞争力，
> 以及这些国家
> 如何能在创新上
> 超过其它国家。

“维基解密”是一种新社会现象的极端之例。这种现象是，致力于将政府公开作为让民众实现自由的方式的组织兴起。

这些组织多数还不到主张披露军事秘密的地步，但都积极推动政府透明度的大幅提高。例如，许多国家要求所有政府官员公开私人财产以防止腐败。中国也正在讨论做类似的事情。

“维基解密”只是众多这类组织中的一个。饱受批评的黑客组织——“匿名者”(Anonymous)也有类似的目标，只不过，它的对象主要是私营企业。该组织相信，私营企业若不将自己所有的信息公开，最终只会做出有碍普通民众自由的事情。该组织的一些成员还相信，企业的创新应该免费让所有人分享，这样能缩小甚至消除贫富之间的差距。

事实上，互联网对数千个这样的组织和网站的发展壮大起到了帮助作用。这些组织和网站相信，保障自由的最佳途径不是选举、法规和法律，而是所有国家中一切组织的信息可以方便无碍地获得。

它们中的一些使用常规的法律途径去获得这类信息。其它更多，包括极端的“匿名者”和“维基解密”，则使用黑客技术。总体上，大多数组织并不极端，但会利用到不同形式的黑客技术。

这个在全世界范围内兴起的运动，我们不妨称之为“解密者”运动。

看待这个问题的一个方式是将国家划分为黑客国家和“被黑”的国家。但这个角度存在问题：正如我们发现，多数国家都在实施黑客行为（尽管多数都予以否认）。

另一种看问题的角度正在兴起，这种看法不把国家分成“黑”与“被黑”两类，而是将公民与运动(超越国家概念)分为“黑客”与“解密者”两类。前者努力想通过获取政府与企业的秘密信息缩小军事与社会差距，后者则努力想通过公布他们所能获得的任何秘密来缩小军事与社会差距。

黑客通常代表的是现状，这些人目前已握有一些权力。解密者主要代表的是下层阶级，他们指向对与错，为那些没有权力、资源、财富或得到三者之一所需信息的人实现公平。解密者是一支正在兴起的力量，他们在像“推特”这样的微博中有很多。而你却不怎么见黑客露面，因为他们是维持现状的秘密力量。

互联网的发展促进了黑客与解密者的发展，但后者的发展更为迅猛。这是因为，黑客是专业而且有偿的，而解密者通常是非专业而且无偿的，因此在数量上也会更多。

黑客、解密者与创新

黑客寻找能利用的创新，但只限于为了自己，而不是他人。解密者也寻找创新，但会将创新分享给其他人。因此，黑客最终限制创新，因为他们将创新限制在一小群组织中间，独自获取财富并雇佣更多黑客，而解密者刺激创新，因为他们一旦发现创新就会传播。

专门以商业为目标获取其它企业新想法和创新的黑客，反映出其雇主创新的速度不够快，甚至缺乏创新。基本上，他们因为无力自己开发所以通过盗取来弥合自己在创新上的差距。

美国企业整体上不会用黑客技术获取其它国家公司的商业秘密，部分由于法律的限制，还有部分原因在于它们的创新速度已经尽可能地快了。美国的教育体系有利于培养企业家与创新者，因此美国企业可以源源不断地获得人力资源，保证美国的创新机器不断迅速向前。可以说，美国的企业不需要黑客（尽管偶尔还是有黑客事件发生）。

在中国，创新则面临许多强大的制约。其中包括重视一致性和考试多于跳出常规思维的教育体系，以及儒家思想对等级与年龄的敬重。这样的条件利于以黑客作为创新途径的滋生。

在中国，许多条件同样不利于解密者。当然，解密者在美国也遭到很多反对，但他们有更多法律与社会的保护。因此，来自解密者的创新在中国也不存在。

这对中国的创新而言并非好事。黑客技术可以获得创新，但创新只局限于一小群人，而不会在社会上广泛传播，迅速作用于许多人；中国的教育与社会环境又不利于创新的发展；解密者虽然在适当的环境下可以产生变革性的影响，但在中国也受到了强大的制约。

近期发生的黑客口水战事实上并非关乎国防、军事或商业机密，也非关乎法律及道德，真正重要的是，它反映出实施黑客行为的国家在社会与经济上的竞争力，以及这些国家如何能在创新上超过其它国家。

本报记者 兰晓萌 编译

李逵，绰号黑旋风，善使一对板斧。原为江州牢房一个小狱卒，后跟随宋江上梁山。李逵为人率直莽撞，对待宋江情义深重，江州一见即甘愿随侍，最后自愿饮下宋江的毒酒与其共同赴死。李逵武艺高强，嗜杀成性，劫法场救宋江、戴宗时，一马当先，逢人便杀；背母上山时，在沂岭怒杀四虎；赚朱仝上山时，杀死无辜的小衙内；三打祝家庄时，他杀死扈太公一门老小。他是农民阶级坚定反抗腐朽社会的典型代表，是下凡扫除世间恶人的天杀星。

"Hackers versus Leakers and the Significance for Global Innovation"

Dr. E. Ted Prince
Founder and CEO
Perth Leadership Institute
www.perthleadership.org

China Times (Beijing)
March 2013

The Hackers

It is now clear that most large US companies as well as US government agencies are routinely being hacked. US reports blame the Chinese government for a large part of this. US reports are even showing the Shanghai building where the some of the hacking originates and they have even published a name and photo of one of the hackers, an employee of the People's Liberation Army.

But if I were the Chinese government, I would hack the US too. Who knows what the US might do on the issue of the islands? It would surely be important for China to know this.

But it's not just China. There have also been numerous reports of hacking of US financial institutions by Iran. That wouldn't be surprising since the US is currently waging economic war on Iran.

No doubt every country that views the US as being an enemy, or even a possible threat, will have been hacking US private and government organizations. After all, the US is the world's top military power by a long shot. Why wouldn't these countries try to protect themselves? So hacking by China isn't surprising; it would actually be more surprising if it wasn't doing this.

And we can't assume the hacking of US organizations is just being conducted by enemies of the US. It's almost certainly being done routinely by its friends. Israel comes to mind, but we can't assume that other countries such as the Europeans aren't doing the same thing either. Even if they view themselves as being allies, they still want to know what the US is doing and thinking to prepare themselves for possibilities which are not being openly discussed.

Above all, we know that the US is hacking other countries. That certainly includes China. We even know from which buildings in the US some of this hacking is coming from. It isn't impossible that the US hacking of China is even more extensive than the Chinese hacking of the US. In fact it is very likely that it isn't just the scale of US hacking of China that is huge; it's probably its sophistication also. It probably goes way beyond what even China believes the US is doing.

For evidence, just look at the experience of US hacking in Iran. We know that the US and Israel jointly hacked Iranian industry and industrial centrifuges with highly sophisticated digital viruses that heavily damaged some of Iran's enrichment program. That's just what we know about. What don't we know about? Probably much, much, more.

So without any doubt the US is giving as good as it gets. You don't get to be the top military power without being pushy.

The face of defense is not just fighter jets and aircraft carriers. The cutting edge is digital and hacking.

But there are really two main objectives of hacking. One is military. The other is commercial.

The reports in the US suggest that much of the China hacking is aimed at stealing US commercial information and technical secrets. Probably this is correct.

I would imagine that numerous other countries are also doing the same thing. When you are the top innovator in the world, everyone wants to get your commercial secrets. Even if some of this activity is not legal or ethical, it's probably not illegal, at least not everything.

And I think there is even some social and commercial value in other countries hacking the commercial secrets of US companies. It enables them to catch up faster, for their citizens to become richer and therefore to be able to buy more things, including from the US. So probably everyone gains from commercial hacking, although the US companies whose commercial secrets are hacked would probably not agree with me.

But there is one thing we should note. Probably most countries are hacking the US military. There would also be many countries hacking US commercial organizations, but there would be less of these. That is because, in countries with a strong rule of law, employees could sue their employers if they know their company is hacking US commercial secrets. So most developed countries would not be hacking US commercial secrets, although a few would be, in intense secrecy.

And while the US government is without any shadow of a doubt busily hacking Chinese military secrets, we can be pretty sure that US companies are not hacking the commercial secrets of other countries including China. That is because of the fact that under whistleblowing laws in the US, any employee has a financial interest in publishing this fact and could sue his employer with the help of the government. So no US company would do this unless it is very small and privately-owned. The vast majority of US companies would not dare to this.

So the US is probably bigger than any other country in military hacking by a long shot. But in the area of commercial hacking it's probably pretty small.

The Leakers

Ever heard of WikiLeaks? That's the website run by Australian gadfly Julian Assange. Its mission is to open up all government secrets to all citizens of all countries. Its belief is that citizens can't be free unless they have total access to all internal government communications. That includes military secrets. WikiLeaks has published millions of pages of US military secrets and is committed to hacking to find more.

WikiLeaks is an extreme example of a new social phenomenon. That phenomenon is the rise of people who are committed to open government as a way of achieving freedom for their citizens.

Most of these organizations don't go so far as advocating that military secrets be exposed. But most are committed to a lot more transparency in government. For example, many countries require that all government officials make all their private assets public so that any corruption can be exposed and prevented. China is discussing doing the same thing.

WikiLeaks is only one of many of such organizations. The infamous hacker organization Anonymous is also committed to the same cause except that it focuses on companies in the private sector. Its belief is that unless you make all their information totally open, private companies will end up doing things which deny ordinary citizens their freedom. Some of their members also believe that innovations from one company should be given for free to anyone who can make use of them, so that the gap between the rich and the poor can be reduced or even eliminated.

In fact, the Internet has spawned the proliferation of thousands of organizations and websites committed to open information from companies and governments. These websites believe that freedom is best guaranteed not by elections, rules and laws but by totally free access to any information by any organization in any country.

Some of these organizations use normal legal means to get access to these types of information. Many others, including extreme ones such as Anonymous and WikiLeaks, use hacking to get access to this information. Most organizations are not as extreme as these but still use various forms of hacking.

We will call this movement, the Leakers. These are the organizations, websites, and citizens who believe that open access to all information is the best way to address abuses of freedom by governments and companies and to narrow the gap between rich and poor.

One way of viewing countries is to divide them between the Hackers and the Hacked. The problem is, as we have seen, that most countries are engaged in hacking (although most deny it), at least for military if not commercial reasons.

There is another way to view the world as it is emerging now. This is to see it not as two types of countries, the Hackers and the Hacked. The other way is to view it as being divided into two types of citizens and movements, independent of countries, namely Hackers and Leakers. Hackers try to narrow military and social gaps by getting access to secret information in government and companies. Leakers try to narrow military and social gaps by publishing anything secret they can find.

Hackers usually represent the status quo, those who hold power currently. Leakers represent the underclass. They are aiming to right wrongs and achieve equality for those who don't have power, resources, wealth or the information to get any of these. So Leakers are an emerging revolutionary force. Leakers are heavily represented in microblogs like Twitter. You don't usually see the Hackers at all because they are a secret force to uphold the status quo.

The growth of the Internet is leading to the growth of both Hackers and Leakers. However Leakers are growing much faster. This is because Hackers are professionals and paid. Leakers are usually amateurs and unpaid so there are vastly more of them.

Hackers, Leakers and Innovation

Hackers aim to find innovations that they can then use themselves, but they get them only for themselves, not for others. Leakers also aim to find innovations but then they give them to everybody. So Hackers ultimately limit innovation by keeping them within the small group of organizations that alone have the wealth to employ Hackers. Leakers stimulate innovation because once they find any, they spread them to everybody.

Hackers who focus on commercial targets to find new ideas and innovations reflect a situation in which their employer either is not innovating fast enough or not innovating at all. Basically they are trying to narrow the innovation gap by stealing the information since they cannot develop it themselves.

US companies generally don't hack the commercial secrets of overseas companies partly because it's very easy for them to get sued by their employees and the government. But partly they do it because they are already innovating as fast as they can. The US education system supports entrepreneurs and innovators so there is plenty of raw human material coming into US companies to keep the US innovation machine moving ahead quickly. So US companies don't really need Hackers (although occasionally they do this anyway).

But there are various powerful constraints on innovation in China. One is the education system which emphasizes conformity and exams over out-of-the-box thinking. Another is the Confucian reverence for hierarchy, rank and age. So conditions in China and countries like it favor Hackers as a way of innovating. That's because there might be no other choice given social and educational constraints.

And conditions are not favorable for Leakers either in China. Of course, even in a place like the US there is a lot of opposition to Leakers. But they have legal and social protections that are not available in China. So the innovation that could come from Leakers isn't present in China either, even though we can see that conditions may be emerging for this to happen.

That is not a good omen for innovation in China. Hacking can find innovations in other countries but they won't be spread widely enough in society to make much difference quickly to a lot of people (as distinct from making the small group of people who employ hackers very rich) and in any case the social and educational systems severely limit innovation processes. Leaking can have a transformational impact in the right circumstances but is unlikely to have much, if any impact in China for social and political reasons.

The issue regarding hacking targeted at the US isn't really about defense, military or commercial secrets. Nor is it about the legality and ethics of taking them from another country or company. It's really about what it reflects about a hacker country's social and economic competitiveness relative to other countries, and how well it can out-innovate them.

That's how Americans – and Chinese – need to judge the significance of the hacking targeted at the US.

Dr. E. Ted Prince, the Founder and CEO of the Perth Leadership Institute, located in Florida in the US have also been CEO of several other companies, both public and private. He is the author of 'The Three Financial Styles of Very Successful Leaders (McGraw-Hill, 2005) and numerous other publications in this area. He is a frequent speaker at industry conferences. He works with large corporations globally on leadership development programs and coaches senior executives and teams in the area of financial leadership. He has held the position of Visiting Professor at the University of Florida in the US in its Graduate Business School and also at the Shanghai University of Finance and Economics in China.