Publication: Asian Scientist Online
Date: 5 February 2018
Headline: A Head For Hacker-nomics

A Head For Hacker-nomics

Unraveling the economics of cyberattacks is just as important as grasping the technologies that hackers use to launch them, says SMU Assistant Professor Wang Qiuhong.

AsianScientist (Feb. 5, 2018) – By Sim Shuzhen – Just as a thief planning a bank heist must figure out how to open locks, bypass security cameras and make a quick getaway, a hacker must also devise ways of cracking passwords, circumventing intrusion detection systems and concealing his electronic traces. The difference is that while the thief's reach is limited in physical space, the hacker can inflict damage across international boundaries from a computer in a remote location.

Virtual in nature and global in reach, cybercrime is a very different beast from crime in the physical world, and fighting it has proved to be an uphill battle. Still, the good news is that cybercriminals are not a completely unknown quantity—just like their counterparts in the real world, their actions are often rational and motivated by economic incentives. Therefore, looking at cybersecurity through the lens of economics could help researchers come up with better countermeasures against online threats.

Taking this very approach is Assistant Professor Wang Qiuhong of the Singapore Management University (SMU) School of Information Systems, who uses tools from economics to study a range of public policy and business issues related to cybersecurity.

"I think cybersecurity is not just a technical issue, but also a business and economics issue. We need researchers who can cross disciplines, and who deeply understand the technology as well as the economics and social science," she says. "They can then bring these disciplines together and gain insights that will facilitate decision making."

A punishment that fits the crime

To deter conventional criminals, governments pass laws and impose penalties on those who flout them. But due to the unique, transboundary nature of cybercrime, it is unclear whether or not legislation actually deters hackers from launching attacks, says Professor Wang.

Together with her collaborators, Professor Wang has used economic modelling to assess how effective the Convention on Cybercrime (COC) has been at deterring distributed denial of service (DDOS) attacks. Introduced in 2001 and now signed by more than 50 countries, the COC is the world's first piece of international legislation against cybercrime.

Using data from real attacks in 106 countries, the researchers showed that enforcement of the COC was associated with a nearly 12 percent decrease in DDOS attacks; this effect, however, disappeared when the enforcing countries were unwilling to fully engage in international cooperation. Professor Wang and her collaborators published their results in a 2017 paper in MIS Quarterly, titled 'Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks'.

Publication: Asian Scientist Online
Date: 5 February 2018
Headline: A Head For Hacker-nomics

"Whether legislation can deter cyberattacks may seem like a very intuitive question, but it can have a very important impact on the government's decision making," says Professor Wang.

Her study not only provides evidence that legislation, international collaboration and enforcement can indeed deter cyberattacks; more importantly, it also shows that the effectiveness of the same piece of legislation can vary from country to country depending on the details of how it is implemented, she explains.

But the picture can get even more complicated. Despite its impact on overall cybercrime rates, legislation seems to be less effective at deterring hackers who are intent on acquiring the capability to launch cyberattacks on a large scale, says Professor Wang.

"In this scenario, hackers are compromising a computer not for the purpose of destroying a system, but to leverage its computing power, storage capacity and connectivity to launch more serious attacks targeting other networks and computers," she explains.

Thus, cybercrime countermeasures should not be limited to reducing the frequency of attacks or to protecting the targets of these attacks, says Professor Wang.

"It is equally important to reduce the severity of attacks and to weaken the attackers' acquisition of capabilities to launch attacks," she explains.

Location, location, location

In the real world, a country has geographical neighbours; in cyberspace, it has what Professor Wang calls topological neighbours—countries through which its data packets are routed as they make their way around the World Wide Web.

This brings a fundamental economic principle into play: that of externalities. When a country and its topological neighbours have made comparable efforts to implement cybersecurity legislation, they are likely to experience positive externalities that reinforce the effectiveness of that legislation, leading to a reduced risk of cyberattacks for all parties. On the other hand, if one country implements effective legislation while its topological neighbors let hackers run riot, this mismatch in cybersecurity capabilities may result in negative externalities, leading to an increased risk of cyberattacks, explains Professor Wang.

"When addressing issues of deterrence, we have to be aware of how our [topological] location will affect our cybersecurity countermeasures, and also how our countermeasures will affect other countries," says Professor Wang.

These relationships, she adds, could be very different from conventional geographical, political or economic ties. One of her current projects is therefore to understand the connections between cyberattacks and the structure of the internet; this, she hopes, will help countries and businesses devise strategies to position themselves in more secure topological locations.

The fight against cybercrime looks set to be a long-term struggle, says Professor Wang.

"Digitisation and the internet have made everything easier. But when we open these doors to legitimate businesses and day-to-day activities, it also opens doors for hackers and criminals," she muses. "The need for cybersecurity is a by-product of our technological advancement."

Thus, rather than simply reacting to the latest malware attack, authorities would do better to seek an in-depth understanding of the fundamental nature of cybercrime from a longitudinal perspective, says Professor Wang.

"It is always important to ask where we are, where we are going, whom we will impact and who will impact us, and to constantly review cybersecurity policy in light of that information."

Publication: Asian Scientist Online
Date: 5 February 2018
Headline: A Head For Hacker-nomics

Asian Scientist Magazine is a media partner of the Singapore Management University Office of Research & Tech Transfer.

———