3-2017

Are the trade-offs for reducing cross-border cybercrime manageable?

Steven Mark MILLER
Singapore Management University, stevenmiller@smu.edu.sg

Qiu-Hong WANG
Singapore Management University, qiuhongwang@smu.edu.sg

Robert John KAUFFMAN
Singapore Management University, rkauffman@smu.edu.sg

Are the Trade-Offs for Reducing Cross-Border Cybercrime Manageable?

Published in Brink Asia March 28, 2017

http://www.brinknews.com/asia/are-the-trade-offs-for-reducing-cross-border-cybercrime-manageable/

Steven Miller Vice Provost (Research) at Singapore Management University

Qiu-Hong Wang Assistant Professor at Singapore Management University's School of Information Systems

Robert J. Kauffman Professor of Information Systems at Singapore Management University's School of Information Systems

Keywords: Cybersecurity, Innovation, International Crime, Privacy

Without increased government intervention and government-industry collaboration, the advantages inherent in the next wave of Internet-enabled digital transformation will increasingly tilt toward cybercriminals, and their influence will disproportionately increase.

The dilemma that immediately presents itself in such a scenario, however, is that an increased level of government involvement can also lead to undesirable consequences. Increasing security always comes with trade-offs that must be managed. The obvious concerns relate to the erosion of privacy, illegal or extralegal persecution, the abuse of Internet censorship and the impediment to or stifling of innovation.

Recent Breaches

Some Asian countries have been especially active in contributing to cybercrime.

The recent large-scale cybersecurity breaches caused by Mirai botnet attacks provide a good example of the seriousness of cyber threats. Since October 2016, Mirai and its variations have been responsible for massive distributed denial of service (DDOS) attacks across the globe, causing large-scale Internet outages for millions of users. The confirmed incidents include attacks against a DNS service provider in the U.S., and various broadband service providers in Europe.

In late October 2016, successive waves of cyber attacks, consisting of massive DDOS attacks powered by Internet of Things (IoT) and peripheral devices that were compromised, brought down the broadband network of one of the leading telcos in Singapore, causing several hours of Internet outage and a disruption of services for subscribers. The specific source of this cyber attack was not publicly disclosed or confirmed. Some observers in the media noted the similarity to the Mirai attacks that had just previously occurred in the U.S. Singapore's Computer Emergency Response Team (SingCERT) released an advisory on enhancing the security of Internet-connected devices right after the attack. The Mirai malware and related attacks in the U.S. were mentioned in the SingCERT advisory, but there was no specific link to the attack that had just occurred.

A joint statement by the Singapore government's Cyber Security Agency (CSA) and Infocomm Media Development Authority indicated that this was the first time that the telco infrastructure in Singapore suffered from such a serious attack. On December 3, 2016, subscribers of another Singapore telco's

island-wide broadband network experienced an outage lasting over 12 hours. The company said this outage was unrelated to the Mirai attack, but has not disclosed the reasons for the extended outage.

Need of the Hour

In doing rigorous academic analysis of how national cybercrime enforcement measures and polices influence and mitigates cybercrime occurrences, we have found several useful, publicly available data sources for determining how national cybercrime policies, law and enforcement measures influence cybercrime occurrences. Additional sources of data are also available to professionals with appropriate qualifications and contacts. However, there are many other important data sources for examining these relationships that are only available to those with high security clearance working in government or at a telecom service provider.

Based on the academic analysis noted above, we have concluded that governments need to be more actively and deeply involved in protecting the Internet from cybercriminals.

In the Mirai botnet attacks, Internet service providers (ISPs) were put in embarrassing and potentially dangerous situations. As they are digital intermediaries, members of the public in each country usually assume that ISPs in that country are liable for their subscribers' information security when they face cyber attacks.

ISPs act as gatekeepers to detect and filter malicious traffic, and they are sometimes able to quarantine infected facilities and networks before the impacts of hackers reach their subscribers. During the Mirai botnet attacks, timely countermeasures taken by the affected companies mitigated attacks and prevented customers' information from being further compromised. Similarly, timely countermeasures taken by the Singaporean telco during and immediately after its attack mitigated damages and consequences.

Who Pays?

Serious efforts to contain and reduce globalized cybersecurity risk require more substantial and sustained investment. But who is going to make these investments? All Internet traffic passes through ISPs, so one obvious answer is that the ISPs should be the ones making this investment. However, most ISPs have slim profit margins and also face high infrastructure costs and an aggressive competitive environment. While ISPs have been investing to deal with cyber attacks, the investment levels are not large enough; and while ISPs may have the desire to do more to protect against cyber attacks, there's no economic incentive for them to do so.

The Internet can be regarded as a "digital commons" where all participating users need to invest in order to maintain adequate security. In such circumstances, where infrastructure is viewed as being a common "public good," it has long been known that the key economic principles associated with its management need to involve a third party beyond the participants. This is where the government needs to come in.

The government is able to address information security in two critical ways: by facilitating infrastructure protection and end-user protection, and by developing and strongly enforcing laws that reduce incentives for attackers to perpetrate disruption and crime online.

Governments' role in deterring cybercriminals is particularly important given the global and virtual nature of cyber attacks. When the Mirai botnet attacks occurred, various information-security agencies detected eight active command and control (C&C) servers that sent attack commands to the botnets. These servers dynamically used 57 different IP addresses located in 16 countries. Tracing the sources of the attacks and collecting electronic evidence of the wrongdoing required collaboration efforts across all 16 of these countries. But there were obstacles to doing this—not all the countries had ratified an internationally harmonized legal framework incorporating dual criminality, accessibility to stored computer and traffic data, and extradition and mutual assistance between nations. This substantially reduced the effectiveness of the cross-border investigation effort.

That said, there is increasing cooperation internationally to achieve such coordination and harmony. For example, 53 countries have signed and ratified the Convention on Cybercrime (COC). It represents the first international legislation to address global cybercrime.

A recent study focused on the efficacy of the COC, and including data from 106 countries, showed that enforcement of the COC was related to a decrease in DDOS attacks by nearly 12 percent, but this kind of deterrence effect did not materialize when the enforcing countries were not willing to engage in full international cooperation.

Security Versus Privacy Trade-Offs

The examples of closer collaboration across governments illustrate that national authorities are beginning to step up to a new level of leadership in cyberspace. Carefully crafted government regulation, as well as closer government-industry collaboration, does, in fact, make the world's cyberspace safer and more trustworthy.

Yet, with increased government scrutiny, there is the risk of reduced privacy, persecution, censorship and preventing innovation.

There are no easy solutions to these trade-offs. Given that governments have already been intervening in domestic and cross-border matters related to the security of cyberspace and will continue to do so due to national security concerns, perhaps it is just as well that we more publicly clarify the rules and mechanisms for how this government intervention is happening.

Without active government involvement, we will not be able to substantially reduce cybercrime. The challenge is to find internationally coordinated ways of addressing cybercrime without causing undesirable consequences.

One publicly announced consequence of the Mirai attack is that Hackforums.net responded to public pressure and permanently shut down its "Server Stress Testing" section, as this was the forum where Mirai's source code was first made publicly available. These shutdowns can be double edged. While they make it less convenient for people with mischievous intent to gain access to malicious code for launching attacks, they also make it less possible for legitimate security professionals to obtain information they need to prevent attacks or to contain them in a timely fashion. Following the countermeasures taken in multiple countries, the scale of the Mirai botnet attacks seems to have diminished. However, suspicious traffic that has been generated by its variations can still be seen.

In the seemingly never-ending battle against cyber attacks, our recommendation is that governments in Asia should go beyond the essential steps of strengthening cybercrime laws and increasing the severity of cybercrime punishment.

Additionally, Asian governments should more actively participate in cross-country collaboration networks for cyberspace monitoring and cybercrime deterrence, investigation and response.

It is important that these increased linkages across national cybersecurity agencies proceed with acute awareness of each country's respective public concerns for privacy, legal protection, censorship and barriers to innovation.