12-2020

# Driving cybersecurity policy insights from information on the Internet

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

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

Robert H. DENG
*Singapore Management University*, robertdeng@smu.edu.sg

# Driving Cybersecurity Policy Insights from Information on the Internet

Qiu-Hong Wang, Steven M. Miller, and Robert H. Deng | Singapore Management University

Published in IEEE Security and Privacy Magazine, 2020, 18 (6), 42-50

https://doi.org/10.1109/MSEC.2020.3000765

Cybersecurity policy analytics quantitatively evaluates the effectiveness of cybersecurity protection measures consisting of both technical and managerial countermeasures and is inherently interdisciplinary work, drawing on the concepts and methods from economics, business, social science, and law.

The battle between cybersecurity protection and perpetration will never be settled on account of human beings' intrinsic motivation for interconnection in modern society. First, information technology-enabled interconnections bridge the existing system and network boundaries across countries, organizations, and people. The rapid penetration of interconnection results in ever-emerging vulnerabilities embedded in the creation of new technologies and new uses of existing technologies. Second, cybersecurity threats are a by-product of freedom and prosperity empowered by digital transformation, as they manifest themselves in the routine activities of everyday life. The extensive digital presence within social activities and personal assets substantially increases the opportunity of the convergence of suitable targets and motivated perpetrators in space and time. Third, the dual-use nature of cybersecurity technology further catalyzes the arms race between techniques adopted for civilian and commercial purposes and techniques exploited for security violation,1 with examples found in the evolution of technologies for cryptography, remote access control, and resilience testing. The social, economic, and technological roots of cybersecurity determine that effective national cybersecurity policies are as important as technical countermeasures in tackling cybersecurity threats.

Cybersecurity policy analytics contributes to improving the effectiveness of cybersecurity policies by identifying the relevant mechanisms and deriving the business and policy implications underlying the emerging risks associated with advanced technologies. One of the key issues in conducting cybersecurity policy analytics is the availability of panel data to support a causal inference that relates the precursors and drivers of observable outcomes through various kinds of processes. In this article, we first discuss three critical empirical inquiries arising from challenges to the effectiveness of cybersecurity policies. Then we introduce how multiple-sourced data sets have been found and integrated to support quantitative measurements and causal inferences in initial efforts, which attempt to answer the three critical inquiries. The results we report are based on two types of empirical studies:

■ We use backscatter data to address the deterrence challenges of law enforcement against cybercrimes. We make use of visible and identifiable backscatter traffic on the public-peering infrastructure of the Internet.

■ We use online hacker forums on the surface web. These types of data are used to analyze the censorship dilemma related to public online hacker forums and consider the benefits of law enforcement shutting down such forums versus allowing them to operate in the open. They serve as a suitable means for sharing the knowledge and tools used for protecting against cyberattacks, or perhaps in the opposite direction, for committing cyberattacks.

We further propose the potential of using Internet routing data to address the interdependence of cybersecurity across national or organizational boundaries. Finally, we discuss the future directions and challenges involved in cybersecurity policy analytics research.

## Three Critical Empirical Inquiries Related to the Effectiveness of Cybersecurity Policies

Similar to conventional crimes, a national government can address cybercrimes from the perspectives of perpetrators, victims, and intermediaries.[1] The first-party strategy aims to deter cybercriminals through either legal or cost deterrence. Legal deterrence imposes sanction costs ex-post offenses. Cost deterrence criminalizes computer misuse acts (CMAs) ex-ante offenses (e.g., the production, distribution, and possession of computer misuse tools with offensive intent) to raise the barrier to acquiring the techniques and tools used for committing cyberattacks. The second-party strategy facilitates user precaution by subsidizing cybersecurity investment and promoting cybersecurity information sharing and emergency response. The third-party strategy leverages the power of intermediaries by imposing secondary liability upon them or motivating their provisioning of cybersecurity services. The intermediaries include a broad range of Internet service providers, cloud service providers, software vendors, and hardware manufacturers that supply the infrastructures and platforms used for interconnection and digitization.

Both private- and public-sector organizations are more actively seeking help from their respective national government authorities to reduce incoming cybersecurity threats and facilitate cross-border coordination for threat monitoring, detection, and resolution. However, the effectiveness of government measures is subject to the challenge of the unique characteristics of cybercrimes, mainly from the three following aspects.

First, cybersecurity perpetrators use cost-effective means that are empowered by cheap computing power and ubiquitous Internet connections. The remoteness, invisibility, and anonymity pertaining to cyberattacks further increases the cost of monitoring and investigating offenses, which, in turn, reduces the success rate of enforcement.[1] Such concerns about the difficulty of deterrence lead to an empirical inquiry about the deterrence effect of law enforcement against cybercriminals. Second, the dual-use nature of cybersecurity technology implies that, to develop a defensive capability against cyberattacks, there needs to be a deep understanding of an adversary's technology and mindset. Thus, criminalizing the production, distribution, and possession of computer misuse tools with offensive intent may deter the provision of hacking techniques intended for cybersecurity violation and, at the same time, generate the unintended effect of discouraging information sharing about similar techniques and vulnerabilities for civilian purposes. Consequently, the cost of deterrence on cybercriminals leads to an empirical inquiry about the net effect of the communication of hacking techniques on cybersecurity threats and the extent of overdeterrence on legitimate cybersecurity professionals.

Finally, the cybersecurity of any individual entity in an interconnected system depends not only on its own effort but on the efforts exerted by other entities in the same system and the infrastructure or platform related to them. The positive externalities of cybersecurity investment across interconnected users and organizations indulge cybernegligence, while the negative externalities of cybersecurity risks among them dampen the private interests for cybersecurity precaution. The interdependent risks, together with interweaving infrastructures and systems, render the efforts of any individual entity (either individual or organization) in cybersecurity prevention technically and economically inefficient.[2] Hence, to evaluate the impact of any cybersecurity policy, we must take into account the interactions among the entities in the cybersecurity ecosystem. This, in turn, leads to an empirical inquiry on the quantitative measurement of the evolution of the infrastructure and/or platforms that are underpinning the interconnected business and social activities, which have been missing in previous empirical studies due to data unavailability. In the following sections, we introduce the initial efforts that address the aforementioned three critical empirical inquires via publicly accessible information on the Internet.

## Difficulty of Deterrence

The main purpose of crime legislation and enforcement is to deter potential criminals via criminalization and punishment. Deterrence through legislation and enforcement has been challenging in the realms of cybercrime because perpetrators can utilize the remoteness, invisibility, and anonymity of online activities and leverage their cost advantages when committing cyberattacks. By spoofing their source IP addresses, controlling remotely located compromised computers, or additionally turning remote computers into attacking botnets, attackers can anonymously conduct malicious activities and victimize computer systems all over the world. Tracing back to the original attackers often requires collaboration between organizations and countries to use preserved stored computer data and network traffic data for forensic analysis. Dual criminality and extradition treaties are additional requirements to prosecute and convict international suspects. Because of all these difficulties in unambiguously pinpointing the perpetrator and in implementing cross-border enforcement, the extent of the deterrence effect of cybercrime legislation has long been questioned.[1]

Moreover, attackers can undermine or thwart legal investigations and enforcement by switching targets, restructuring attack paths, and relocating the attacking resources for the purposes of avoiding detection and maximizing criminal returns. Hence, imposing penalties on the commission of cybercrimes may sometimes lead to criminals changing their behavior in ways that cause unexpected, negative results. According to the theory of marginal deterrence,[3] law enforcement may divert perpetrators to other victims with a higher profit margin or to jurisdictions with weaker enforcement. Perpetrators may even vary the frequency and severity of attacks to render the monitoring and investigation costs associated with enforcement too costly to proceed. In this article, we introduce three studies that address the deterrence effects of law enforcement from the following research questions:

- Does domestic enforcement deter cyberattacks?[4]
- Does international legislation deter cyberattacks?[5]
- Does international legislation lead to marginal deterrence, or does it fail in this respect?[6]

In these studies, the data assembled on cyberattacks have been linked with assembled data from global news sources on cybercrime enforcement and with compiled data on country-specific cybercrime legislation and international cybercrime treaty agreements. For international treaty legislation, the focus was placed on the Convention on Cybercrime [(COC); Europe Treaty Series No. 185], which was the first international legislation against cybercrime and has 55 allied member states as of April 2020.

## Cyberattack Data

To measure the cyberattack rate and its severity, these studies obtained the backscatter data that was sent by distributed denial of service (DDOS) attack victims and made available by the Center for Applied Internet Data Analysis [(CAIDA) 2005–2019] and the Internet Storm Center (2004–present). The backscatter traffic manifests itself in terms of visible and identifiable traffic on the public-peering infrastructure of the Internet. It is the cyberattack data set that has the longest monitoring and reporting history (since 2000 to the present for DShield data) and the broadest coverage (with victims geographically located in more than 200 countries). Both data sources have worldwide coverage with detailed attack information. By tracking the backscatter packets and their origins, it was possible to analyze the change in DDOS attack victims and in the severity of attacks at a granular level over time and across organizations.

## Enforcement and Legislation Data

To identify any government enforcement actions against cyberattackers, Png et al.[4] searched the contents of Factiva, a subscription database owned by Dow Jones & Company, Inc., a subsidiary of News Corporation,

which provides access to 33,000 global news sources including licensed publications and influential websites and blogs, images, and videos. Keywords related to hacking, conviction, jail sentence, and prosecution in the official language for each country were used to search the Factiva database.

Various international organizations maintain country profiles on cybersecurity development and cybercrime legislation. For example, the International Telecommunication Union (ITU) publishes a cyberwellness profile that provides an overview of a country's cybersecurity development, including its legal measures. However, as the ITU acknowledges, "No single publication can adequately cover all aspects in depth." Accordingly, Hui et al.[5] have compiled lists of cybercrime domestic legislation in each country from multiple sources, including information from the Asian School of Cyber Laws, the Council of Europe, the ITU, and the United Nations Office on Drugs and Crime. Once relevant domestic legislation was identified, they conducted further search via the Internet to locate—to the extent possible—more detailed information on each country's legislation, including details on dates of entry into force and changes in legislative content or items.

To investigate the causal effects of law enforcement on cyberattacks, the event study methodology originally used in financial economics and the difference-indifference methodology founded in quantitative social science research have been adapted to identify the change on cyberattack rates as a direct result of government legislation and enforcement, relative to the countries and/or the time periods without enforcement. In particular, the autonomous system (AS)-level peering partnership across country borders has been used to measure interdependence in terms of Internet traffic. An AS is one of the most important components of Internet infrastructure. Referring to Request for Comments 1930, "An AS is a connected group of routers run by one or more network operators, which has a single and clearly defined routing policy." The AS relationship data are provided by CAIDA on a monthly basis. The utilization of AS-level peering data empowers Hui et al.[5] to identify the reinforcement effect and displacement effect of the COC resulted from the Internet traffic interdependence across ASs originating from different countries.

Figure 1(a) and (b) illustrates the reinforcement effect of the COC. A hacker's real geolocation is AS1 in country A and targets victims' infrastructure within AS4 and geolocated in country D. AS2 and AS3, geolocated in countries B and C, respectively, are AS4's Internet peering partners who transit data traffic originating from or delivered to AS4. Hackers remotely control the zombie networks in AS2 and AS3 to commit DDOS attacks targeting victims in AS4. Figure 1(a) shows that if country C is a non-COC country, a hacker can always conceal their real location by conveying a DDOS attack via the zombie networks within AS3 geolocated in country C, given countries A, B, and D are all COC countries. As country C is not a COC country, it has no obligation to provide the necessary resources and information to facilitate COC countries in cybercrime investigation, which makes the hacker's attack path untraceable. Figure 1(b) shows that when all of AS4's Internet peering partners, AS2 and AS3, are geolocated in COC countries, all the attack paths targeting AS4 are trackable, which increases the hacker's prosecution risk and results in a deterrence effect against hackers.

Figure 2 illustrates the displacement effect of the COC. Under the same situation as in Figure 1(a), where only country C is a non-COC country, hackers may relocate their zombie networks from AS3 in country C to AS4 in country D and substitute the original victim in AS4 with a new victim in AS3. Because AS3 is geolocated in a non-COC country, the law enforcement agency in country C is unable to acquire the necessary information from either country B or D to trace back the hackers' real location. Hence, the DDOS attacks targeting victims in AS3 may increase as all of its Internet peering partners except AS3 itself are geolocated in COC countries. These studies provide insight into the deterrence effects of law enforcement from three aspects.

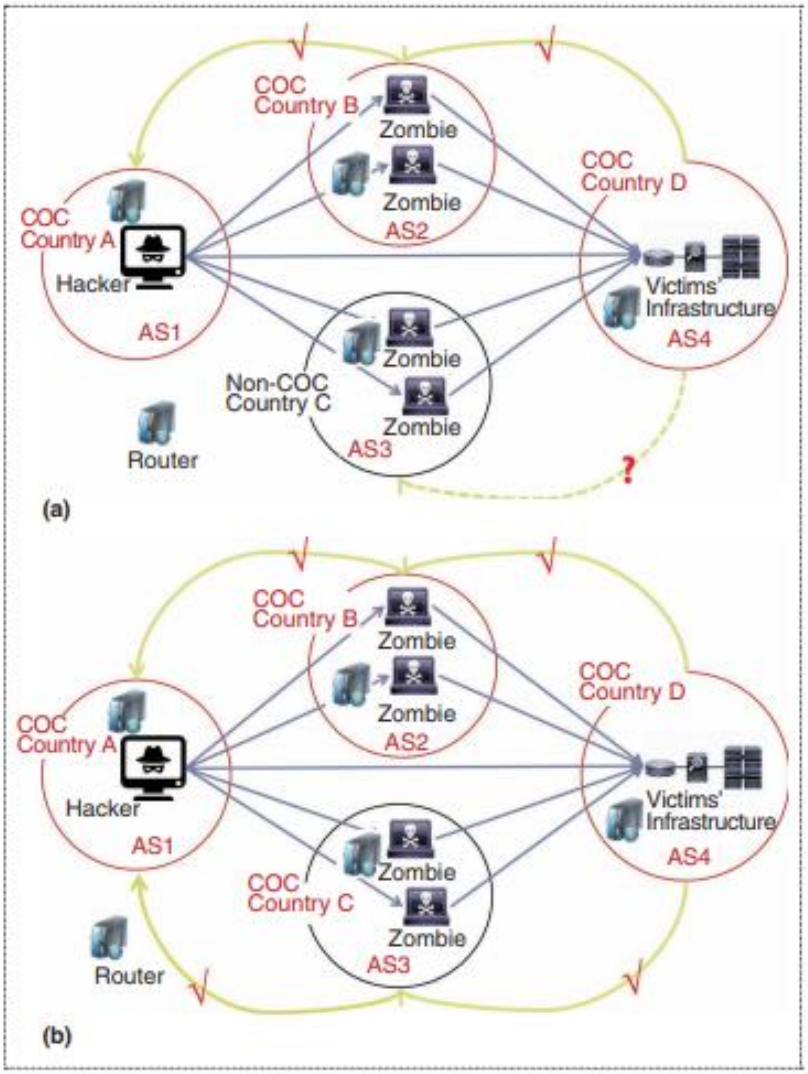


**Figure 1.** The reinforcement effect of the COC via (a) and (b) Internet peering partners.

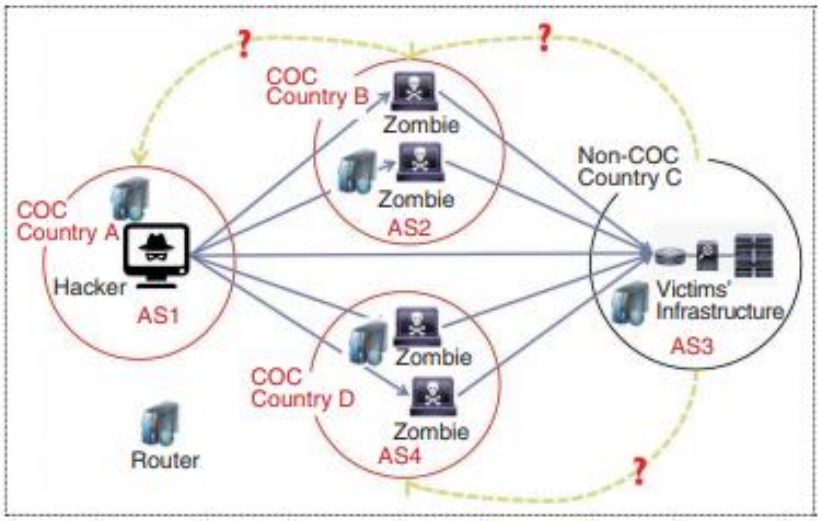


**Figure 2.** The displacement effect of the COC via Internet peering partners.

**Domestic Enforcement**

They found limited evidence that domestic enforcement deters attacks within the country; however, they found compelling evidence of a displacement effect: as the enforcement of U.S. cybersecurity laws strengthened, more attacks were originated from overseas locations.[4]

**International Legislation**

They found evidence of successful deterrence by the international COC legislation. The number of IP addresses victimized by DDOS attacks decreased by at least 11.8% in the enforcing countries. This deterrence effect did not exist, however, when the enforcing countries were not fully abiding by all the requirements of the treaty. In other words, in those countries that were abiding by the treaty to only a limited extent, the decline in the number of cyberattacks was a smaller percentage decrease or was nonexistent. These studies also found evidence of network and displacement effects. The enforcement was particularly effective when other countries also fully enforced the COC. At the same time, this may result in cyberattacks being displaced to other countries not participating in the treaty or to those not fully abiding by it.[5]

**Marginal Deterrence**

They found that, although the number of IP addresses victimized by DDOS attacks tended to decrease in the new COC countries, the severity of the attacks, as measured by the maximum number of bits per second targeting each IP address, systematically increased in these countries. This finding suggests that although the COC could deter minor attackers, determined attackers may pursue more serious attacks given the expected penalty. Hence the failure of marginal deterrence does exist in cybercrime enforcement.[6]

Future research on the law enforcement of cybersecurity offenses may extend in two directions. The first direction is to study the strategic responses between organizations and attackers by leveraging the organizational level backscatter traffic and the Internet peering data on a daily or even hourly basis. This requires extra efforts to link IP addresses or AS numbers with their affiliated organizations, and further, to integrate with business databases widely available for listed companies, venture capital funds, or intellectual properties. Such an interdisciplinary integration of data on cyberattacks and of Internet peering and business data sets using public IP addresses or AS numbers as the linkage, may generate innovative and insightful business and policy implications for cybersecurity management.

The other direction is to study the impacts of law enforcement on other types of cyberattacks with distinct technical mechanisms compared to DDOS attacks. For example, looking at publicly accessible large-scale cyberincident data feeds on spam emission and phishing website hosting. The available data sources include Composite Blocking List, Passive Spam Block List, and many other Domain Name System-based blackhole lists of suspected email spam sending computer infections. Free phishing feeds are also available in OpenPhish, a fully automated self-contained platform that collects and analyzes millions of unfiltered uniform resource locators from a variety of sources on its global partner network. As different cyberattacks involve different cost structures on the perpetrator side and cause different levels of harm on the victim side, an empirical investigation on deterrence effects in various cybersecurity risk contexts could help policy makers understand the economic incentives behind user precaution and criminal offenses.

**The Dual-Use Nature of Cybersecurity Technology**

It is clear and broadly acknowledged by (most) governments, companies, and individuals that malicious attacks that intentionally disable or degrade networks or steal someone’s personal information are wrong and constitute a criminal act. But what about the publicly accessible online discussion of hacking knowledge? Is it

wrong to allow such forums to exist in the open? Should discussing hacking knowledge in publicly accessible online forums be considered the production, distribution, and possession of computer misuse tools with offensive intent and thus subject to the enforcement of a country's CMA? This is not a clear-cut judgment because of the "dual-use" characteristic of these hacking forums.1 The know-how generated and explained in these forums can be used for both malicious purposes (how to launch attacks) as well as for beneficial purposes (how to defend against or respond to attacks).

Both sides of this argument have been put forth. On the negative side, it has been noted that online hacker forums expose more people to hacking and hence promote aggression and copycat criminal behavior, and may also encourage like-minded hackers to collaborate on attacking other people. On the positive side, some have suggested that the discussions in online hacking forums help those looking for ways to protect against or respond to ongoing cyberattacks to acquire the necessary detailed knowledge for protecting themselves or for taking countermeasures to respond more quickly. Another observation is that more open discussion of hacking removes its novelty, which is arguably a major motivator for many "script kiddies." More open availability of hacker knowledge may contribute to establishing stronger and better social norms, which is one way to curb cybercrimes.[1] In the context of these contradictory influences, two focal questions have been examined relative to whether or not publicly accessible online hacker forums should be censored:

■ What is the net impact of hacking discussions in online hacker forums on cyberattacks?[7]

■ How does the banning of such hacking discussions in public online forums influence knowledge sharing of cyberprotection knowledge?[8]

The two questions are related to one another: if the net impact of hacking discussions on cyberattacks is insignificant or even negative, allowing hacking discussions in public online forums should not increase cyberattacks. On the contrary, banning hacking discussions would reduce the exposure of hacking techniques to the public, thereby also eliminating access for law-abiding forum readers to an important source of information on how to protect against such attacks. Unlike malicious and criminal attackers, law-abiding IT and cybersecurity specialists are less likely to acquire hacking techniques via private channels or underground markets. Thus, the public's cybersecurity awareness and protection capability may even decrease if protection-oriented techniques and alerts are not easy to access.

## Hacking Technique-Sharing Data

In contrast to underground hacker communication channels (i.e., an instant-messaging system), hacker forums on the surface web are publicly accessible communities in which a vast amount of user-generated content can be retrieved on a longitudinal basis. These forums differ from the hacker communities on the darknet where participation is by invitation only and most of those invited are black hats who intend to engage in illicit trading. Although publicly accessible forums may not capture the most malicious activities in hacker communities compared to what is happening on the darknet, they are more likely to attract less determined hackers or the curious because of relatively easy entry and low legal risk. Publicly accessible hacker forums represent important cybersecurity forces with the potential to convert hacking techniques into defensive measures as well as the potential to join professional hackers in committing cybercrimes. Indeed, publicly accessible hacker forums are vantage points from which we can observe the variety of discussions on cybersecurity techniques. These discussions display a spectrum of intent ranging from offensive to neutral to defensive, which provides an ideal setting for investigating the emergence of various interests on hacking techniques and the impacts of national cybersecurity policies on them.

Six well-known and representative hacker forums in English, Chinese, and Russian were selected for content analysis with a focus on cybersecurity techniques. Latent Dirichlet allocation models, various supervised learning models, and manual classification were used to classify millions of hacker forum posts comprising a mixture of programming scripts as well as unstructured and casual textual discussions.[7]

Among various hacking techniques, DDOS attack techniques are chosen because of the availability of real-world attack data and their association with specific port numbers. The discussion of DDOS attacks within the six hacker forums was linked to real-world DDOS attacks via the Transmission Control Protocol/ User Datagram Protocol (TCP/UDP) port numbers specifically mentioned in the hacker forum discussion that featured DDOS attack-related keywords. These linkages were used to investigate the empirical relationships between online hacking forum discussion and real-world cyberattacks, including rigorous statistical modeling to test for causality (aside from correlation).

Chinese online hacker forums were used to investigate the second research question mentioned previously. The Chinese government enacted Amendment VII of the People's Republic of China Criminal Law on 28 February 2009. The amended Article 285 of Section 3 (we refer to Article 285) criminalizes the production, distribution, and possession of computer misuse tools. It states that "Whosoever provides programs and tools specifically for the purpose of intruding into and illegally controlling computer information systems or provide others with programs and tools, knowing full well that those persons commit illegal and criminal acts of intruding into and controlling computer information systems, where the circumstances are grave, shall be punished for fixed-term imprisonment of between three to seven years." According to Article 285, the discussion of malicious attack techniques is subject to enforcement. Following the enforcement of this amendment, forum administrators were required to remove posts containing hacking techniques and to impose surveillance on user-generated content. The impact of the enforcement of this CMA was addressed by comparing forum users' knowledge contribution before and after the CMA, with the control of confounding effects from group size and online community competition. Figure 3 shows the conversion of users' online discussion topics from cybersecurity-related topics (e.g., a protection- or hacking-oriented discussion, or a neutral discussion on security techniques without specifying a use for either protection or offense) to cybersecurity-irrelevant topics following the CMA enforcement.

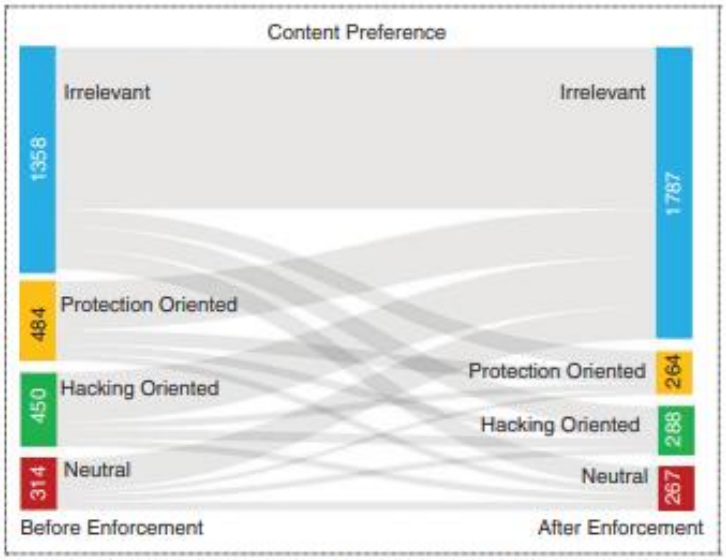


**Figure 3.** How cybersecurity technology interests changed among users registered in two representative Chinese online hacker forums after the enforcement of the CMA in China.

Research based on the aforementioned hacker forums shows that the discussion of DDOS attacks in online hacker forums was associated with a decrease in the number of DDOS attack victims. The mention of botnets, especially new botnets, was initially correlated with an increase in attacks, but the follow-up discussion was mildly correlated with a decrease in attacks. Hence, the discussion in online hacking forums does appear to have the dual-use characteristic noted previously, and as such, the effect of having these types of publicly available forums has both negative and positive aspects.[7]

Enforcement against the production, distribution, and possession of computer misuse tools tended to increase forum contributions on protection-oriented discussions. However, this contribution was mainly provided by users who had originally focused on hacking-oriented discussions as their risk of discussing hacking techniques increased following the enforcement. On the other hand, this enforcement discouraged those contributors who had originally actively contributed to the protection-oriented discussions. This is probably because users' perceived value of protection-oriented discussion increases with their perceived threats from malicious activities. With less discussion of hacking techniques, the forum participants may end up being less aware of the prevalent malicious activities related to cyberattacks. As a result, their interest in protection-oriented discussions also decreases.[8]

These findings support previously published work that noted that these forums have a dual-use characteristic. As such, although the presence of these online hacker forums is problematic in some ways, banning them makes it more difficult, and therefore more costly, for white hats and legitimate users to be alerted to and informed about up-to-date cybersecurity threats and hacking techniques. Banning these forums also pushes black hats and gray hats to underground communities, which are full of illegal transactions and more difficult for legal monitoring and investigation. The existence of these online hacker forums is a double-edged sword for cybersecurity threat reduction and for national cybersecurity policies. Future research in this direction can be extended to various forms of online hacker communities including forums, blogs, and other types of user-generated content. Other than keyword-based feature engineering, advanced natural language processing should be applied here to extract context- and structure-related information based on specific domain knowledge on cybersecurity, information sharing, and social networking. This type of in-depth data preprocessing and coding is the prerequisite to conducting data analytics toward insights with mechanisms rooted in theories of economics, law, and social sciences. Such an interdisciplinary integration of data sources, methodologies, and theories may contribute to the knowledge of social, economic, cultural, and psychological forces in the intertwined evolution of constructive and destructive cybertechnologies.

**The Measurement of Cybersecurity Interdependence**

With Respect to Internet Infrastructure The Internet infrastructure is the physical foundation of digitalization and the most important infrastructure and platform underpinning modern society's interconnected business and social activities. The deeply interconnected nature of network infrastructure and the frequency of deep linkages between hardware and software components contribute to system interdependencies that are not always easily observable and further complicate the assessment of and response to cybersecurity risk.[9]

However, cybersecurity interdependence and its role in the policy implementation of interconnected organizations have seldom been empirically addressed in the field of information systems (IS), which focuses on research about designing, implementing, and managing information technology. We reviewed cybersecurity-related articles published in the top-ranked IS journals and conferences from 2004 to 2019, focusing on identifying the data sets that IS scholars have utilized in their security research. Examples of journals we reviewed are Information Systems Research, Management Information Systems Quarterly, Journal of Management Information Systems, and Journal of the Association of Information Systems. The conference articles we reviewed were from the International Conference on Information Systems and the Workshop on the Economics of Information Security. Our review showed that no Internet infrastructure-related database has been used by researchers publishing in IS literature to address security issues or to measure the underlying nature and degree of organizational interdependence from a network connectivity point of view.

The lack of research in the management and policy-oriented IS community on Internet infrastructure and the related network connectivity and interdependence may be attributed to the invisibility of Internet infrastructure to most end users due to modularization and encapsulation in the layered computing system design. Following up on the work of Hui et al.,5 IS researchers have started to utilize global Border Gateway

Protocol (BGP) routing data to quantify and measure the interorganizational relationships associated with selected cybersecurity incidences.5 BGP routing data consist of millions of feasible routing paths for Internet peering from one AS to another AS. This type of information also includes the rules that routers can read and follow when transiting data traffic from one node of the Internet to another on an almost real-time basis covering most of the publicly available AS numbers and IP prefixes for nearly three decades since the early 1990s [e.g., RouteViews' BGP RIBs (Routing Information Bases), which originated in 1995, is one of the well-established databases used for BGP routing].

Internet peering relationships and their associated Internet traffic exchange are, in essence, a specific way to identify and measure business relationships between organizations. These peering relationships capture interdependence in Internet infrastructure, which underpins the interconnected networks and systems. Thus, we think BGP routing data are one of the richest data sources publicly available to measure cybersecurity interdependence with respect to Internet infrastructure.

In a recent research effort, we quantify the topological characteristics of ASs and their interdependency in Internet traffic.11 The period of provision that we considered ranges from the year 2006 to 2019 on a daily and per-AS-basis level. We develop an AS connectivity index created from the RouteView data for the measurement of AS abnormality, maliciousness level, and the Internet traffic interdependence between ASs. We are able to identify the countries or organizations that may unintendedly become the critical Internet traffic intermediary of another organization. An organization can choose partners with whom to transit or exchange its Internet traffic but cannot control how those partners connect to the rest of the Internet. This constrained business liability may result in unintended interdependence in Internet traffic. Thus, we think that newly generated data sets at the Internet infrastructure level can provide an important step toward the comprehensive measurement of cybersecurity interdependence at different layers of computer network architecture across countries or organizations.

The studies discussed in this article demonstrate that cybersecurity policy analytics can be done using publicly available Internet information. Obviously, the quality, specificity, and relevance of this policy analytics work are dependent on the types and amounts of information that is publicly available to those doing this type of cybersecurity policy work. The pooling of information on cybersecurity incidents contributed by worldwide volunteers provides opportunities to quantify more precisely the differential impacts of government regulations and online activities on real-world cyberattacks. At the same time, the quality and scope of information sharing on threat detection and emergency response have been hampered over the years from insufficient incentives to share this type of information among various participants. This has limited the precision and extent of efforts to date to measure the impacts of cybersecurity legislation on deterring cyberattacks.

We believe that it is crucial to design effective incentive-compatible mechanisms for cybersecurity-related information sharing among organizations by taking into consideration the unique setting of the cybersecurity ecosystem. A higher level of contribution of private organization information on cybersecurity incidents would tremendously benefit the types of cybersecurity policy analytics described in this article. As such, we need to search for incentives for private organizations to make selected aspects of their information available on cybersecurity incidents.

Some promising cases of cybersecurity information sharing have proven successful in the areas of healthcare12 and Internet infrastructure.13 Health-care institutions that join health information exchange (HIE) programs in the United States are obligated to disclose their data breach incidents, which, in turn, motivates these HIE participants to implement strong information technology governance to reduce data breach risks. Internet or network service providers that connect to Internet exchange points (IXPs) have to share and update their real-time network traffic and routing information among IXP participants to enable and benefit from public peering, which, in turn, enhances IXP participants' capabilities for monitoring and detecting the malicious traffic exchanged between their Internet peering partners.

As proposed by Wang and Geng,[13] in both cases, cybersecurity-related information sharing is not initiated by the needs of cybersecurity itself but by the intrinsic need for business efficiency. It is indeed the business-driven interest that connects information sharing—a means—and specific cybersecurity goals. This connection, featured with specificity, makes cybersecurity information sharing incentive compatible and operationalizable. Because specific cybersecurity information sharing is based on mutual benefits, it further improves the trustworthiness of the data shared among participants. As such, we suggest that cybersecurity information sharing among private organizations should be initiated, specified, and implemented according to participants' core business values.

The success of cybersecurity information sharing also relies on enhanced, international collaborative and coordinated efforts to collect and process the huge volume of publicly accessible cybersecurity-related information available through the Internet.14 This includes information on vulnerabilities, alerts, and attacks as well as the related forum posts and discussions. Much of this type of information is text based, and each item provides a tiny fragment and localized piece of a much larger and globally integrated puzzle on the status of cybersecurity issues and incidents. Collecting and integrating all of these separate and localized information fragments and transforming them into systematically organized, unified, and quantified data sets greatly expands opportunities to measure and analyze the evolution of cybersecurity vulnerabilities, the interdependency of cybersecurity risks, and the emergency responses to cybersecurity incidents on a global scale.

## Acknowledgments

This research was supported by the National Research Foundation Singapore under grant NRF2016NCRNCR001-009. This article is based on an online technical report https://ink.library.smu.edu.sg/sis_research/4435/ that was first presented by the authors at the Third Digital Research Seminar, the International Criminal Police Organisation Global Complex for Innovation, 14 September 2017, Singapore.

## References

1. N. K. Katyal, "Criminal law in cyberspace," Univ. Pennsylvania Law Rev., vol. 149, no. 4, pp. 1003–1114, 2001. doi: 10.2307/3312990.

2. C. Hall, R. Anderson, R. Clayton, E. Ouzounis, and P. Trimintzios, "Resilience of the internet interconnection ecosystem," in Economics of Information Security and Privacy III, B. Schneier, Ed. New York: Springer-Verlag, 2013, pp. 119–148.

3. D. Mookherjee and I. P. L. Png, "Marginal deterrence in enforcement of law," J. Polit. Econ., vol. 102, no. 5, pp. 1039–1066, Oct. 1994. doi: 10.1086/261963.

4. P. L. Png, C. Y. Wang, and Q. H. Wang, "The deterrent and displacement effects of information security enforcement: International evidence," J. Manage. Inf. Syst., vol. 25, no. 2, pp. 125–144, Fall 2008. doi: 10.2753/MIS0742-1222250206.

5. K. L. Hui, S. H. Kim, and Q. H. Wang, "Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks," MIS Quart., vol. 41, no. 2, pp. 497–523, 2017. doi: 10.25300/MISQ/2017/41.2.08.

6. K. L. Hui, S. H. Kim, and Q. H. Wang, "Marginal deterrence in the enforcement of law: Evidence from distributed denial of service attack," Research Collection School of Information Systems, Singapore Management University, Aug. 2013. [Online]. Available: http://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article= 4519&context=sis_research

7. W. T. Yue, Q. H. Wang, and K. L. Hui, “See no evil, hear no evil? Dissecting the impact of online hacker forums,” MIS Quart., vol. 43, no. 1, pp. 73–95, 2019. doi: 10.25300/ MISQ/2019/13042.

8. Q. H. Wang, L. T. Zhang, and M. K. Qiao, “Online hacker forum censorship: Would banning the bad guys attract good guys?” in Proc. 50th. Hawaiian Int. Conf. Systems Sciences, Hawaii, Jan. 4–7, 2017. doi: 10.24251/ HICSS.2017.677.

9. Q. H. Wang and S. H. Kim, “Cyber attacks: Cross-country interdependence and enforcement,” in Proc. 8th Workshop Economics of Information Security, Cambridge, U.K., June 2009, pp. 1–17.

10. Y. Zhuang, Y. Choi, S. He, A. C. M. Leung, G. M. Lee, and A. B. Whinston, “Information disclosure and security vulnerability awareness: A large-scale randomized field experiment in Pan-Asia,” in Proc. 53rd Hawaii Int. Conf. System Science, 2020, pp. 1–11. doi: 10.24251/HICSS.2020.739.

11. Q. H. Wang, “Using BGP data for cybersecurity policy analytics,” unpublished.

12. L. T. Zhang and M. S. Pang, “Does sharing make my data more insecure? An empirical study on health information exchange and data breaches,” in Proc. 40th Int. Conf. Information Systems (ICIS), Munich, Germany, Dec. 15–17, 2019, pp. 1–26.

13. Q. H. Wang and R. B. Geng, “Does interconnection increase or decrease cybersecurity threats? An empirical study of organizations connecting to the Internet eXchange Points,” unpublished.

14. S. H. Kim, Q. H. Wang, and J. Ullrich, “A comparative study of cyberattacks,” Commun. ACM, vol. 55, no. 3, pp. 66–73, Mar. 2012. doi: 10.1145/2093548.2093568.

**About the authors**

Qiu-Hong Wang is an assistant professor in the School of Information Systems, Singapore Management University. Her research interest focuses on cybersecurity policy analytics. Wang received a Ph.D. from the National University of Singapore. Contact her at qiuhongwang@ smu.edu.sg.

Steven M. Miller is Professor Emeritus of Information Systems at Singapore Management University. Miller received a Ph.D. from Carnegie Mellon University. Contact him at stevenmiller@smu.edu.sg.

Robert H. Deng is the AXA Chair Professor of Cybersecurity, director of the Secure Mobile Centre, and deputy dean for faculty and research, the School of Information Systems, Singapore Management University. His research interests include data security and privacy, network security, and system security. Deng received a Ph.D. from the Illinois Institute of Technology. He is a Fellow of IEEE and of the Academy of Engineering Singapore. Contact him at robertdeng@smu.edu.sg.