Modern cybercrime policy

Microsoft Policy Papers

Fighting cybercrime in the 21st century

The combination of expanded access to the Internet, the explosive increase in connected devices, and the rapid expansion of innovative cloud-based services is creating tremendous economic and social opportunity for consumers, governments, and businesses. It is also opening up new avenues of attack for cybercriminals and other malicious actors. The consequences are not just economic costs but lost confidence in Internet commerce, the erosion of individual privacy, and diminished trust in online services. Each of these effects threatens to slow adoption of cloud-based innovation and reduce the benefits of promising new technologies.

Governments are struggling to deal with the growing threat, sophistication, and prevalence of cybercrime. It is difficult to develop comprehensive responses to crime that can span identify theft, online scams and fraud, malware distribution schemes, attacks against the integrity of data and systems, and the online distribution of illegal content, to name just a few examples. Moreover, these crimes are increasingly committed by organized groups operating in one country, which target victims in another. The cross-border nature of cybercrime complicates enforcement, and inadequate legal frameworks in some countries have created safe havens for cybercriminals.

A further complicating factor is the pace of development of new technologies. Legal frameworks have traditionally not been outcome focused and can therefore quickly become obsolete, as criminals begin to utilize or attack new technologies, from cloud computing platform to the Internet of Things (IoT). Governments must be able to put forward frameworks that allow rapid responses to new challenges but which also ensure that providers of new technologies and digital infrastructure are not exposed to liability for the criminal actions of others.

In search of effective policy mechanisms

The globalized nature of cybercrime makes *harmonization of cybercrime laws* around the world essential, although this alone may not be sufficient. It is important that such legal harmonization efforts are underpinned by initiatives to facilitate *faster and more effective coordination* between law enforcement agencies. Moreover, these efforts must be pursued in an environment where each country respects the sovereignty of others, and where citizens' fundamental rights and liberties are fully respected.

Microsoft believes that to strengthen enforcement in a balanced way, governments should consider the following steps:

- *Strong enforcement and balanced rules.* To fight cybercrime effectively, law enforcement agencies and technology providers need appropriate legal tools for pursuing cybercriminals wherever they are. Governments can increase the effectiveness of efforts to fight cybercrime by updating criminal statutes to address existing and emerging threats posed by online criminals. These new laws should be designed so that they don't hamper future innovation or slow the adoption of new technologies. Legal frameworks that supports industry self-regulation are also important.

- *Adopt laws that are consistent with broadly accepted international conventions.* The Council of Europe's Budapest Convention provides a good model for cybercrime legislation that harmonizes laws and facilitates better cooperation across borders. Such international coordination and cooperation will help eliminate safe havens for malicious actors and minimize the risk that service providers and other innocent parties are subject to conflicting obligations or liabilities.

- *Facilitate information sharing.* Today, companies that have information about online crimes can face liability under privacy, data protection, or other laws if they voluntarily share information with law enforcement. This

can deter them from providing data to law enforcement agencies that could be critical in preventing or quickly responding to cybercrime. Laws that clarify rules for data sharing and liability can help facilitate timely cooperation between law enforcement agencies and cloud service providers.

- *Adopt enhanced Mutual Legal Assistance Treaties*. Because cybercrime does not stop at national borders, law enforcement agencies in different countries must be able to work together efficiently and according to clear rules. When the victim of a cybercrime is in one jurisdiction, the criminals are in another, and the servers through which the crime is committed are somewhere else entirely, law enforcement agencies need effective standards and mechanisms for rapid cooperation. Strengthening the procedures and mechanisms for international, cross border cooperation through bi- or multi-lateral arrangements will help streamline enforcement efforts and clarify important issues of jurisdiction and access to evidence.

- *Work with industry on best practices and emerging issues.* The private sector offers expertise and resources which governments can use to fight against cybercrime. This can include working with industry to educate enforcement officials on new and emerging threats, given that technology suppliers and their customers often see these first. In addition, governments often struggle with inadequate resources as they work to stay ahead of cybercriminals; by collaborating with the private sector, law enforcement agencies can do more with fewer resources, which in turn will help drive greater trust in online computing.

Criminals and criminality cannot be eliminated from cyberspace any more easily than from the real world. They will adapt and change in response to law enforcement and the precautions of individuals and businesses. Nonetheless, by developing a flexible, outcomes-oriented approach to the regulation of technology, one that takes account of its rapid technical development and the equally rapid evolution of its use, policy-makers can help law enforcers keep pace with criminals’ as they adapt. Furthermore, by facilitating public-private partnerships with the developers and providers of internet, mobile and cloud technologies, the forces of law and order can stay ahead of the curve; able to spot and jointly emerging criminal trends before they become major threats to businesses, citizens and governments themselves.