Is cybersecurity a public or private good?

Keerthi, Gaurav

2023

Keerthi, G. (2023). Is cybersecurity a public or private good?. RSIS Commentaries, 140-23.

https://hdl.handle.net/10356/171629

RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 140 – 6 October 2023

Is Cybersecurity a Public or Private Good?

By Gaurav Keerthi

SYNOPSIS

As digitalisation and technological advancement accelerate rapidly, the issue of cyber space security looms large, and a pressing concern is who should ensure that it is a safe place for the future of our work, play and life. As the roles of government, business, and individual users of digital applications are being debated intensely, the threats are increasing relentlessly, and it is inevitable that the state must exert itself more purposefully for the sake of public interest.

COMMENTARY

The threat of being hacked was once a distant possibility that only big corporations and governments took seriously. Today, even small businesses and ordinary citizens tread delicately in the digital domain, fearful of scams, malware, and other threats that lurk online. It is thus natural for individuals, companies, and states to ask deeper questions about cybersecurity, and how it should be more optimally provided. Defining the role of the private versus public sector may also shed some light on the underlying policy positions of Singapore's 2021 National Cybersecurity Strategy.

Provision of Public and Private Goods

A good starting point is: What are public and private goods?

Public goods include items like street lighting, clean water, and national security; things that are defined as non-rivalrous in consumption (my use of street lighting does not prevent your use of it), and non-excludable (it is difficult to provide street lighting for only one person but not another).

Private goods are both rivalrous and excludable; if I buy the last car in the showroom, you cannot have it or use it. Typically, public goods are provided for in some ways by

the government, while private goods are most efficiently provided for through the free market mechanism, where customers buy things from companies. Determining what type of good cybersecurity is, impacts on how it should be provisioned and how it should be paid for.

How have states dealt with similar conceptual challenges in other domains? According to a 2022 Gallup poll, when you walk down the streets in Singapore at night, a whopping 94 per cent of people feel safe. Homeland security is provided by the police as a public good, to reduce the risk that armed robbers are roaming the streets at night.

I still invest in good locks to protect the inside of my home, but I know what I am responsible for protecting and what I can leave to the police. Likewise for military defence – I do not install missile warning systems on my rooftop because I trust our competent Air Force to protect me from those threats.

In the physical security domain, we have a sensible balance between individual versus state responsibilities. In the digital world, this is not yet true. Companies and individuals are burdened with the full responsibility of protecting themselves from petty hackers to state sponsored attackers. Physical security is provided mostly by the state as a public good while digital security is not.

Water sanitation offers similar lessons. Before modern plumbing, people were entirely responsible for ensuring that their own water was potable; any water-borne disease suffered was their own fault. These diseases moved from being an individual nuisance to a national health crisis. Blaming individuals was easy, but ineffective. Governments today provide access to clean water from the tap as a public good, to avert a national health crisis.

Poor individual cyber hygiene can also rapidly escalate to a national digital crisis. In 2016, the Mirai Botnet attacks used poorly secured Internet-of-Things devices to take down various popular online streaming services. This attack could be replicated on essential services someday.

Blaming users for their weak passwords may be easy, but ineffective at averting the crisis. For citizens who depend on various digital services, it is inconceivable that the state protects them only in one domain (physical) but not the ever-expanding digital one. Singapore's experience with scams and the public pressure for the state to "do more" is illustrative of these expectations. The public wants "clean" internet, straight from the Internet Service Provider (ISP).

Cybersecurity as a Private Good: A Flawed Concept

As the cybersecurity marketplace is already overcrowded with private solutions, why is intervention necessary? Perhaps it is just that users are too stingy to pay for it? Cybersecurity is an example of a product with "positive externalities" – an economic term for something with benefits to third parties not involved in the transaction – and as such, will always be under-consumed by the market, below what is socially desirable.

Ideally, consumers would pay for the “privilege” of preventing a national cyber crisis; they would patch software, use strong passwords, and stop clicking on dodgy links. This rarely happens in reality, and the market alone will not yield socially efficient or optimal outcomes without intervention.

Furthermore, reinforcing the idea that cybersecurity is a private good may lead to other perverse outcomes: “online security is only for the rich; the poor deserve to be breached”. This is not a tenable public policy position, especially as some argue for access to the Internet to be considered a human right.

Cybersecurity as a Public Good: A Win-Win Solution

Even if states agree on providing cybersecurity as a public good, they must decide how they intend to provide for it.

1. Regulatory intervention. The government can mandate that key infrastructure providers must “clean the pipes” to reduce the burden on end-users. This is very similar to the model for water sanitation. The higher cost of doing so could be absorbed by the owner, passed on to customers, or subsidised by the state (or a mix). In Singapore, the Cybersecurity Act requires providers of essential services to undertake significant cybersecurity protection for their systems.

2. Direct provision by state. The government could implement cybersecurity solutions nationally. One example is SingPass, Singapore’s national biometric authentication system, which has been extended to private sector use.

3. Indirect provision. Much like the provision of street lighting, the government can award large contracts to private suppliers to achieve security outcomes or implement security solutions, like the national protective Domain Name System (DNS) that is offered in some jurisdictions. There are many variations within this model, where the government could own and operate, or own but let the private sector operate, or let the private sector own and operate on the state’s behalf.

4. Subsidies for adoption. Tax incentives are a tool used by states to drive certain behaviour; in the context of cybersecurity, corporate tax benefits could be offered to companies who meet certain security outcomes.

The private sector usually stands to benefit from playing a key role, and the government is better able to achieve its socially desired outcome of protecting its citizens and businesses online. It is a win-win outcome.

Singapore's Safer Cyberspace Masterplan 2020 articulates this policy shift implicitly: “*The Safer Cyberspace Masterplan represents the Government’s blueprint … to better protect Singapore and Singaporeans in the digital domain. It focuses on upstream measures to secure Singapore’s core digital infrastructure, safeguard our activities in cyberspace, and empower our population to adopt better cyber hygiene*”.

In other countries, for example, the United States of America, the White House’s National Cyber Strategy 2023 recognises the market failure but does not go as far as Singapore’s position: “*Together, industry and government must … collaborat[e] to*

correct market failures, minimize the harms from cyber incidents to society's most vulnerable, and defend our shared digital ecosystem".

Going Forward

It would be wrong to conclude that the burden now falls entirely on the state. Even if there are soldiers guarding our borders and police patrolling our streets, we should still buy and use our own door locks. States should be clear what "baseline" general cyber protections to provide as a public good, and what individual users must do for themselves. For many users, this baseline may be enough. For others, who require advanced protection against more sophisticated threats, this will need to be complemented by their own advanced "door locks".

Although cybersecurity is a "team sport", this essay argues that the state needs to play an even bigger role than the users. Singapore's Safer Cyberspace Strategy 2020 aptly compared the provision of cybersecurity to that of publicly funded exercise parks to encourage the population to adopt regular outdoor activities to stay fit and healthy. The government can (and should) build the parks, but we still need to go for the jog ourselves.

BG(NS) Gaurav Keerthi is an Adjunct Senior Fellow, S. Rajaratnam School of International Studies (RSIS) in Nanyang Technological University (NTU), Singapore. He was the Deputy Commissioner of Cybersecurity for Singapore and is the Executive Vice President at Ensign InfoSecurity.
