PUBLIC DATA AT RISK:
CYBER THREATS TO THE NETWORKED GOVERNMENT

Ms LIM May-Ann, Managing Director, TRPC Pte Ltd, & Executive Director, Asia Cloud Computing Association (ACCA)
mayann@trpc.biz @eilonwy @accacloud

Govt Dependence on IT Systems

E-government Infrastructure

- National broadband connectivity
- Management Optimization
- Public Management Systems

Online Services

- E-taxes, license and fine payments
- E-voting
- Public tender system
- Applications for public services
- Citizen email

Public Utilities and Critical Information Infrastructure

- Electricity
- Gas
- Water
- Communications
- Media

Open platforms, interconnection, and interoperability have become some of the most important development issues facing government information technology officers.

Types of Info stored by Govts on IT Systems

Public Documents and Information

Sensitive Public Data

Internal Government Communications, Documentation, Email Exchange Data

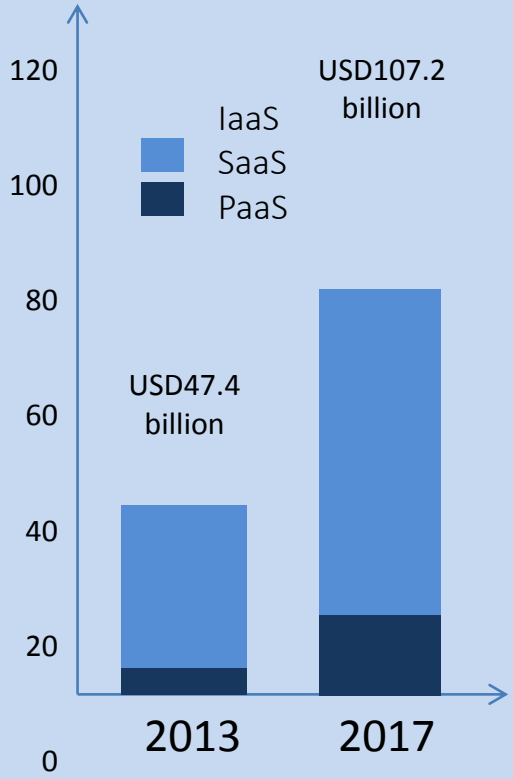
National Security and Defence Information

INTRINSIC DATA	COMMERCIAL DATA	PERSONAL DATA
information created, mined and collated by the government and its agencies	created as a result of transactions and communications between government and the private sector	public data submitted to the government to comply with regulations or to avail of social benefits

Types of Info stored by Govts on IT Systems

> *When large amounts of private government correspondence are released by unauthorized sources – such as in the case of WikiLeaks or the Snowden NSA revelations –* ***the repercussions can be highly damaging to governments involved****.*

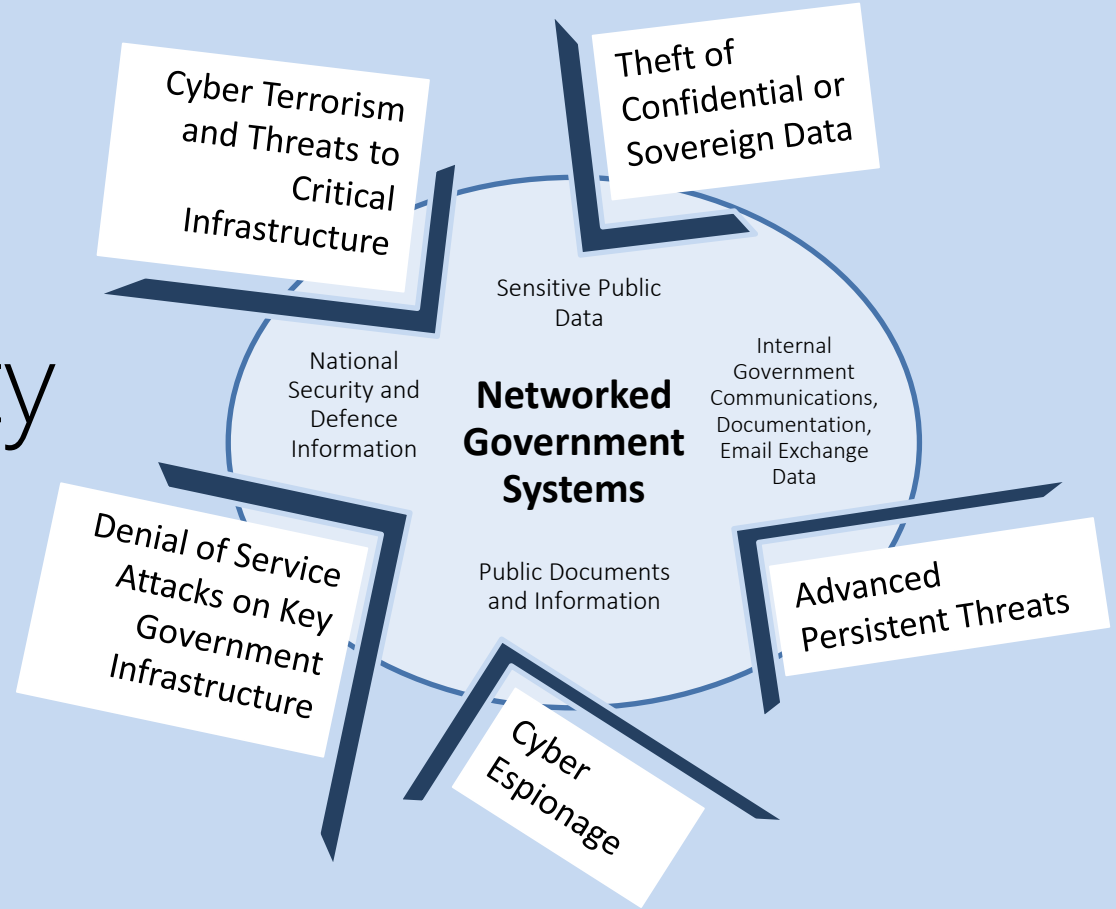
IT Spending by Governments

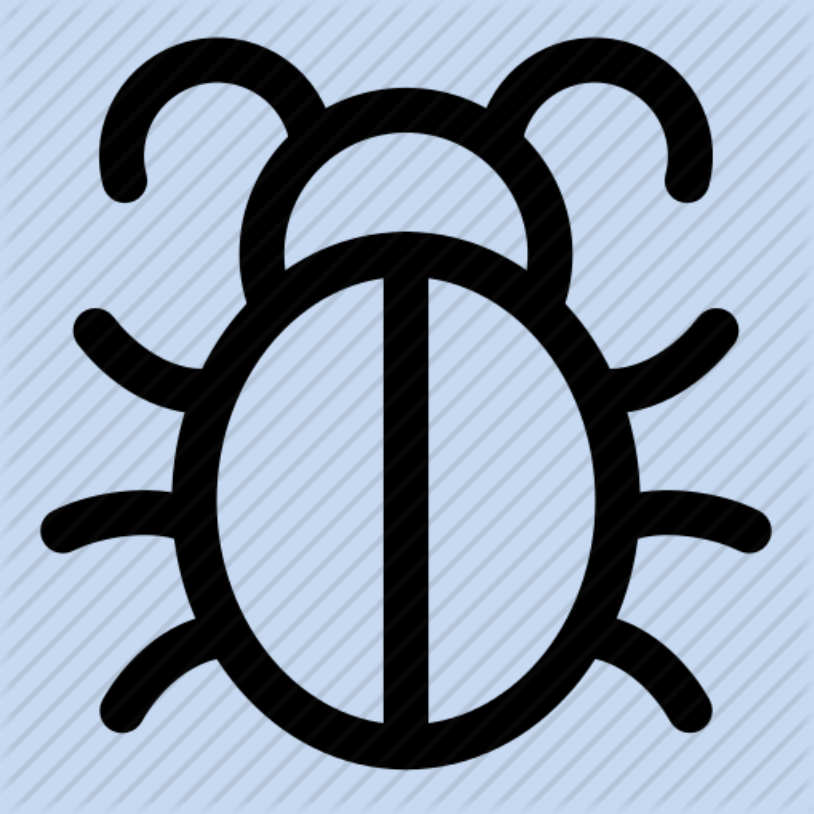


There is a growing understanding that some of these resources must be focused on cyber security issues, especially since ***state-sponsored and state-targeted cyber attacks have been projected to rise.***

“Two problems arise for procurement professionals in Asia – **the rise of infected computers** and the **lack of experience in dealing with actual threats**… (and) most organisations… are not taking enough precautions against the threat of an Advanced Persistent Threat (APT) attack.”

Types of Cyber Security Threats to Govt

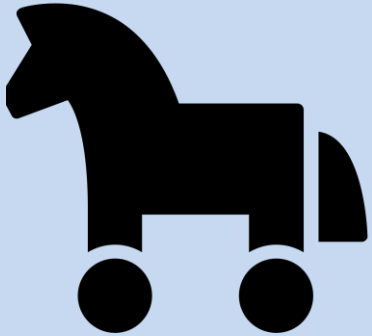




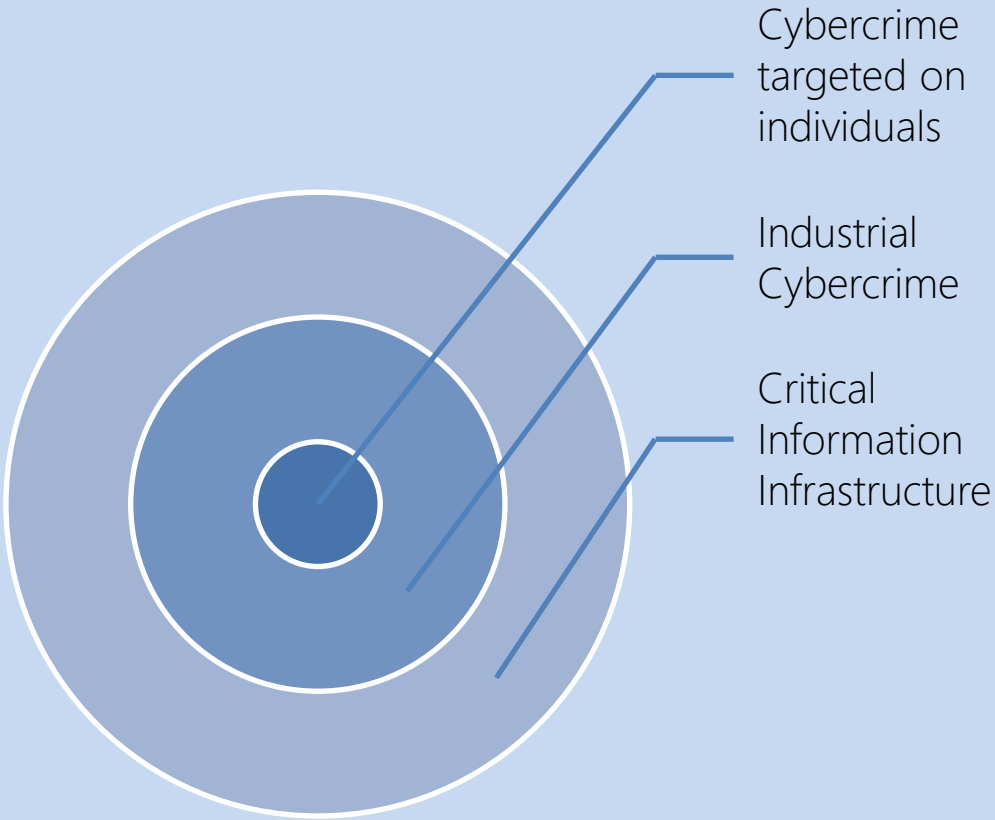
Malware

Malware is software intended to damage or disable computers and computer systems often found on counterfeit or pirated software. These programs create opportunities for hackers by loading malicious code onto computers to gain information and sometimes take control over computers.

- Spyware
- Tracking Cookies
- Adware
- Trojan
- Virus
- Keylogger



Cyber Threat Targets



Roadmap to Creating a Cyber Security Strategy:

Five Components of a Robust Cyber Security Policy

TRPC

Cyber Security Checklist for Govt

What should governments consider or focus on when building a cybersecurity plan?

✓*Awareness and Public Education*

- Have a cyber wellness programme in place for citizens, larger businesses, and SMBs.
- Provide regular training on cyber hygiene to government civil servants. Review the training curriculum regularly (at least once a year) to refresh and keep them up-to-date.
- Review and input to school curriculum, ensuring a basic level of cyber literacy and cyber protection amongst all citizens.

✓*Readiness – Crisis Management Plan*

- Have an agency responsible for coordinating cyber security preparedness and prevention messages.
- Have a single agency responsible for coordinating cyber security responses in the event of a state-targeted attack.
- Establish a Computer Emergency Response Team (CERT).
- Create or join a network of CERT partners to share information, and to work with in mobilisation and mock attack exercises.
- Have a national plan for cyber security in place.
- Identify, meet with and connect critical infrastructure providers (utilities such as power, water, networks) with each other, so as to enable smooth communications and quick responses during a cyber attack.

✓*Prevention – Safe and Protected Network Infrastructure*

- Have a procurement policy (e.g. whitelisting) for authentic software and malware protection in place for government procurement.
- Develop best practices for procurement in place for the private sector, for larger businesses and SMEs.
- Develop cyber security standards for vendors to adhere to before they are eligible to bid for public sector projects.
- Consider the use of cloud computing for best cyber security.

✓*Response – Regulation and Defence*

- Establish domestic, regional and international legal avenues for pursuing redress following a cyber attack.
- Develop best practices for recommended timeframes and standards for constant upgrading and updating software used in the public sector.

✓*Mitigation – Controlling the effects of a Security Breach*

- Establish a cyber forensic team in place which can work alongside the CERT to investigate security breaches.
- Develop or join a cyber security network of other government or international organisations for information and alliance-building purposes.

TRPC