

# Cyber Threat Evolution

## With a focus on SCADA attacks

Anant Shivraj

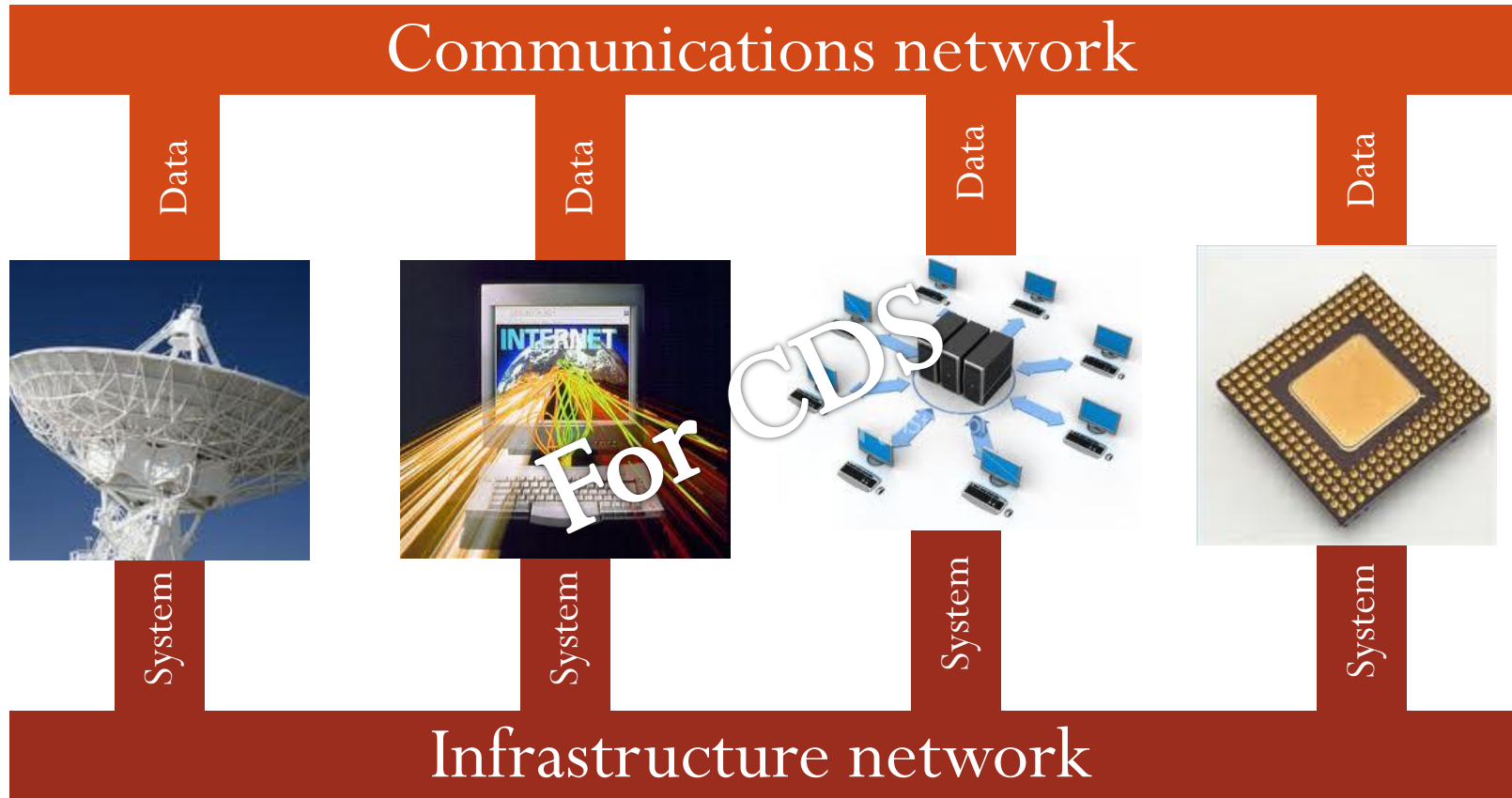
May 9<sup>th</sup> 2011

**Extracts only. For full deck and more information on study,  
contact Center for Digital Strategies/author**

# Agenda

- **Cyber Attacks**
  - **Increasing sophistication of cyber attacks**
  - Private Sector as target of, and medium of attacks
- Vulnerability of the Oil & Gas Industry to Cyber Attacks
  - Profile of risks faced by SCADA systems in Oil & Gas
  - Risk Mitigation Strategies and Effectiveness
- Recommendations

# Cyberspace is more than the Internet



Cyberspace: The interdependent network of information technology infrastructures, and includes telecommunications networks, the Internet, computer systems, and embedded processors and controllers in critical industries.

# Key takeaways from recent incidents

Cyber attacks have evolved from operational events to strategic events, with the aim to disrupt a target's freedom in the real world, not just on the Internet

## Changing Ends

To impact strategic capability and assets

To impede business operations

To target physical assets and mission critical information

## Increasingly Sophisticated Means

Traversing multiple networks and infrastructures

Precision targeting

Multi-stage attacks to avoid attribution

Cyber attacks are employing new techniques such as spear phishing, rootkit for specialist devices and networks, and multi-stage phased attacks to accomplish these aims

# Stuxnet demonstrates a new level of cyber attack capability

- Stuxnet was a worm targeted at industrial control systems (ICS) discovered by July 2010. By then, it had infected upwards of 100K systems in Iran, Indonesia, India and other countries
- Widely believed to have been developed with state support and targeted at Iran's Busheshr nuclear reactor

Symantec W32 Stuxnet Dossier:

*“Stuxnet is a threat that was primarily written to target an industrial control system or set of similar systems.... Its final goal is to reprogram industrial control systems (ICS) by modifying code on programmable logic controllers (PLCs) to make them work in a manner the attacker intended.... In order to achieve this goal the creators amassed a vast array of components to increase their chances of success. This includes zero-day exploits, a Windows rootkit, the first ever PLC rootkit, antivirus evasion techniques, complex process injection and hooking code, network infection routines, peer-to-peer updates, and a command and control interface”*

# Stuxnet demonstrates capability of cyber attacks to harm physical assets

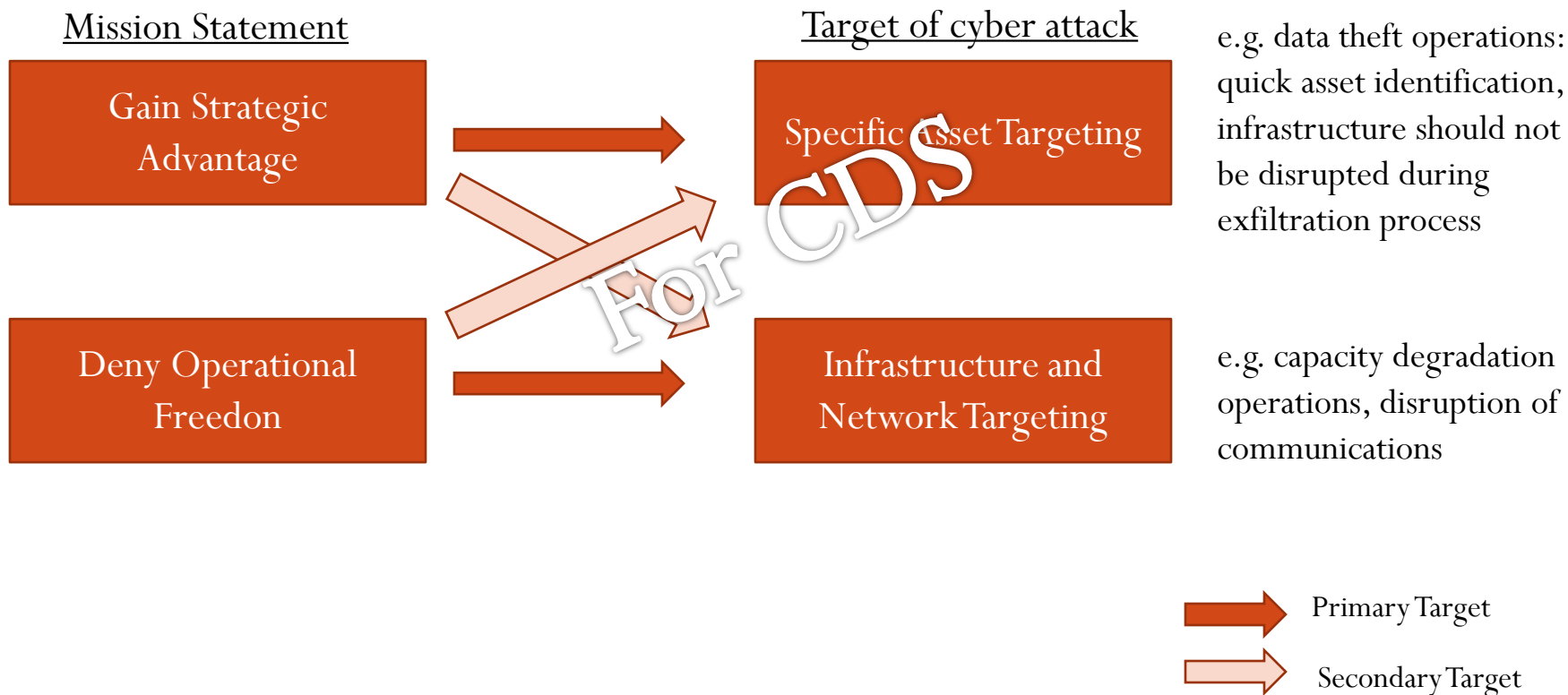
Feature	Comments
Impact	<b>Ability to attack and impair physical infrastructure – industrial data, industrial output, industrial operations in critical infrastructure</b> <b>Stuxnet managed to delay the startup of Bushehr</b>
Key Lesson	Persistent connection to global IP network not essential to be a cyber target
Key Innovations	Precise target selection and anti-virus evasion First PLC rootkit (allowing admin access to PLC functions) P2P self-update capabilities (sleeper Stuxnet worm can auto-update to suddenly attack a host at a later date)
Professional, Coordinated Development*	Projected six months development cycle, 5-10 developers, QA and management Theft of digital certificates, and the need to understand and construct a worm for Industrial Control Systems suggests involvement of multi-disciplinary team

# Two key determinants of cyber attack pathways

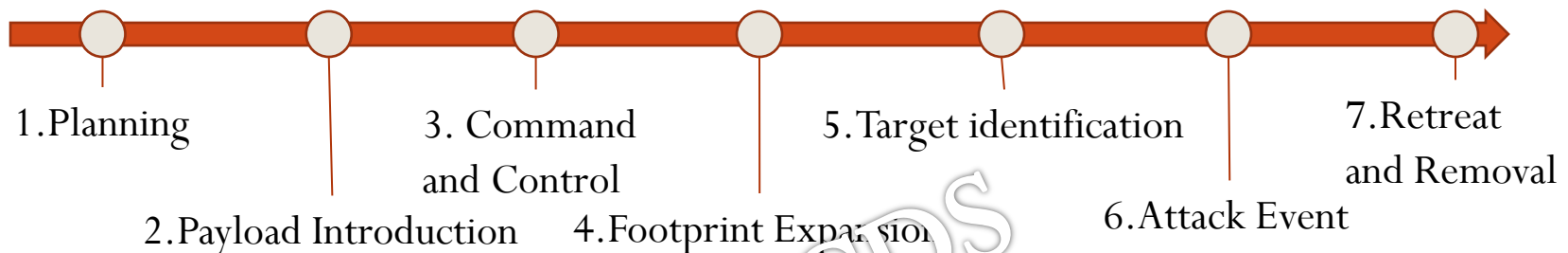
- Mission Statement
  - What the attacker wants to accomplish
  - Depends on who the attacker is
    - Cyber criminals looking for financial gains
    - Non-state actors affiliated with a particular cause
    - State actors trying to accomplish strategic goals
- Technical Capabilities
  - What capabilities are available to the attacker
    - Resources and budget
    - Experience
  - Again, can depend on who the attacker is

**Given that developing technical capabilities has become easier, mission statement is the primary determinant of the attack pathway**

# Mission statement key to which cyber attack pathway is used

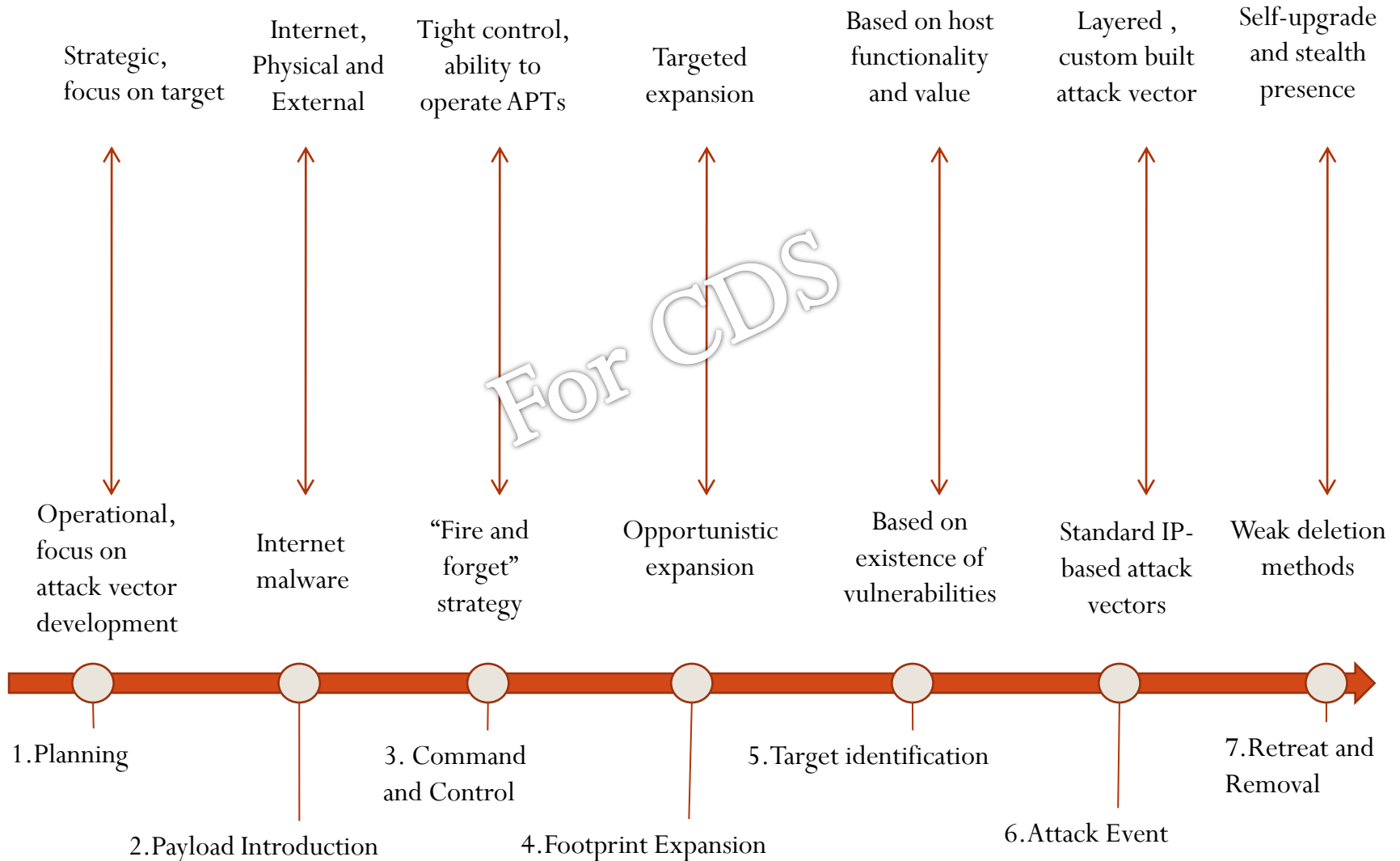


# Seven phases of a cyber attack

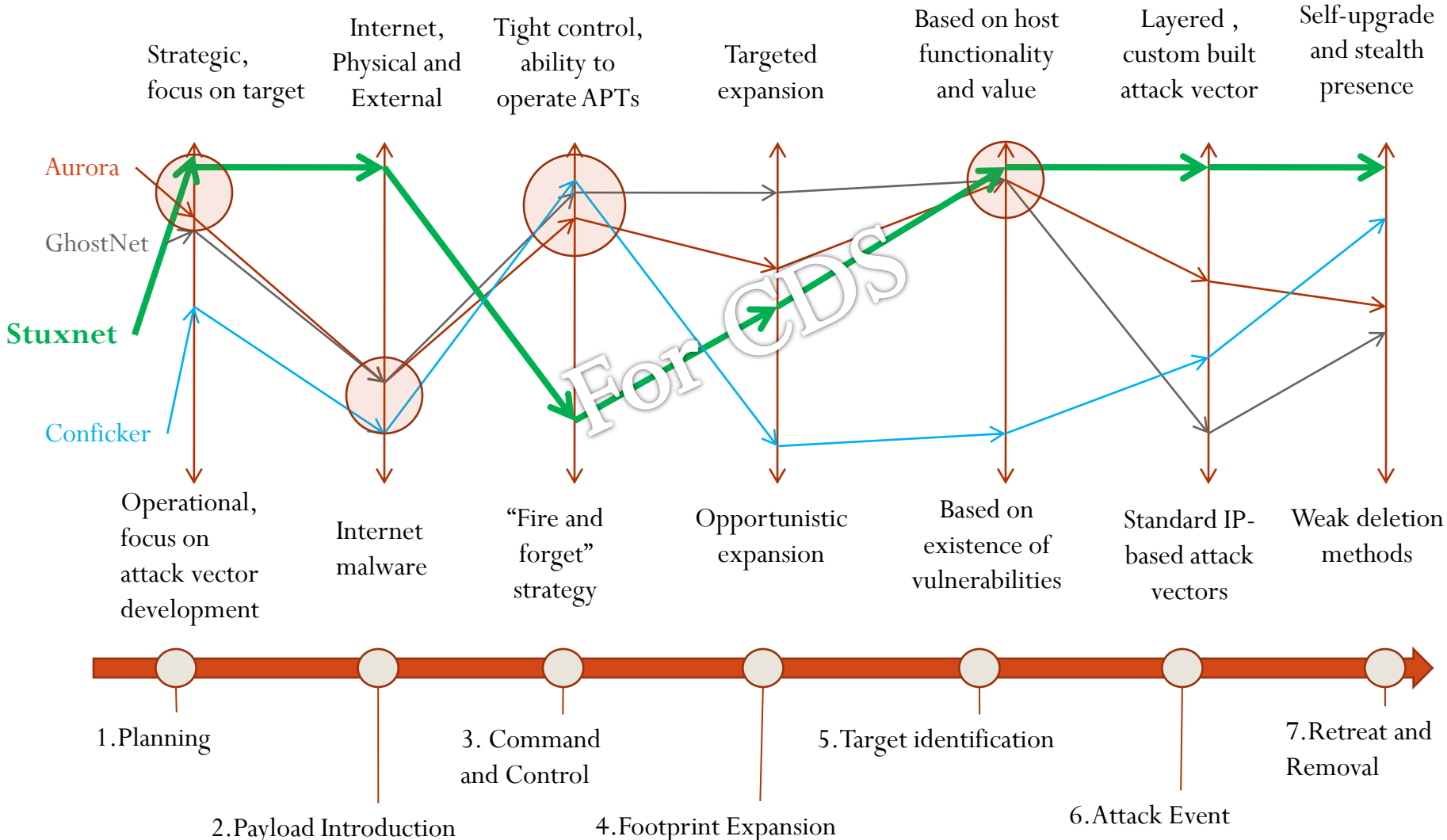


- Starting from the earliest documented worm (“Internet worm 1988”), most cyber attacks have followed a subset of these seven steps
- Most of the above sequence followed by some of the most successful attacks
  - SQL Slammer (January 2003), which slowed global Internet traffic dramatically
  - Conficker (November 2008), which infected 15 million computers and continues to, in spite of industry efforts (and \$250K reward from Microsoft)

# Visualizing attack pathways



# Visualizing recent cyber incidents on attack pathways



○ Indicates increasingly seen characteristics

# Agenda

- **Cyber Attacks**
  - Increasing sophistication of cyber attacks
  - **Private Sector as target of, and medium of attacks**
- Vulnerability of the Oil & Gas Industry to Cyber Attacks
  - Profile of risks faced by SCADA systems in Oil & Gas
  - Risk Mitigation Strategies and Effectiveness
- Recommendations

# Stuxnet used private sector capabilities and targets in its attack on state entity

## Targeted

- **Siemens** Step 7 software compromised via rootkit
- Specifications for frequency controllers from **Vacon (Finland)** and **Fararo Paya (Iran)**

## Exploited

- Digital certificates stolen from **Realtek** and **Jmicron**, which are located in close proximity to each other
- **Microsoft** Windows access gained via rootkit
- Two Internet Explorer zero day exploits
- Domain name servers in Malaysia and Denmark

## Evaded

- Detected and adapted to signature-based and behavioral detection capabilities of 11 anti-virus products including **Symantec**, **McAfee** and **Trend Micro**

# Increasing use of a new capability – spear phishing

Use of highly contextual phishing properties, often sent by known acquaintances, and taking into account real world or online identities, to reduce detection rates

Target	Sent To	Claims to legitimacy
Marathon Oil, ExxonMobil and ConocoPhillips	C-level leadership	Email subject: <i>“Re: Emergency Economic Stabilization Act”</i> (sent after plan had been announced)
Booz Allen	VP for International Military Assistance Prog.	Email subject: <i>“India MCRA Request for Proposal”</i> (India had released RFP a week ago) Sender: <i>from the office of the Air Force Secretary</i>

Increasing spear phishing implies that both signature-based and behavioral virus detection softwares are losing effectiveness, catching only 20% of malware

# Agenda

- Cyber Attacks
  - Increasing sophistication of cyber attacks
  - Private Sector as target of, and medium of attacks
- **Vulnerability of the Oil & Gas Industry to Cyber Attacks**
  - **Profile of risks faced by SCADA systems in Oil & Gas**
  - Risk Mitigation Strategies and Effectiveness
- Recommendations

# Oil and gas sector officially identified as a critical infrastructure

- Critical infrastructure: “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitation impact on security, national economic security, national public health or safety or any combination of those matters.”
- 18 sectors identified as critical infrastructure by the Homeland Security Presidential Directive 7

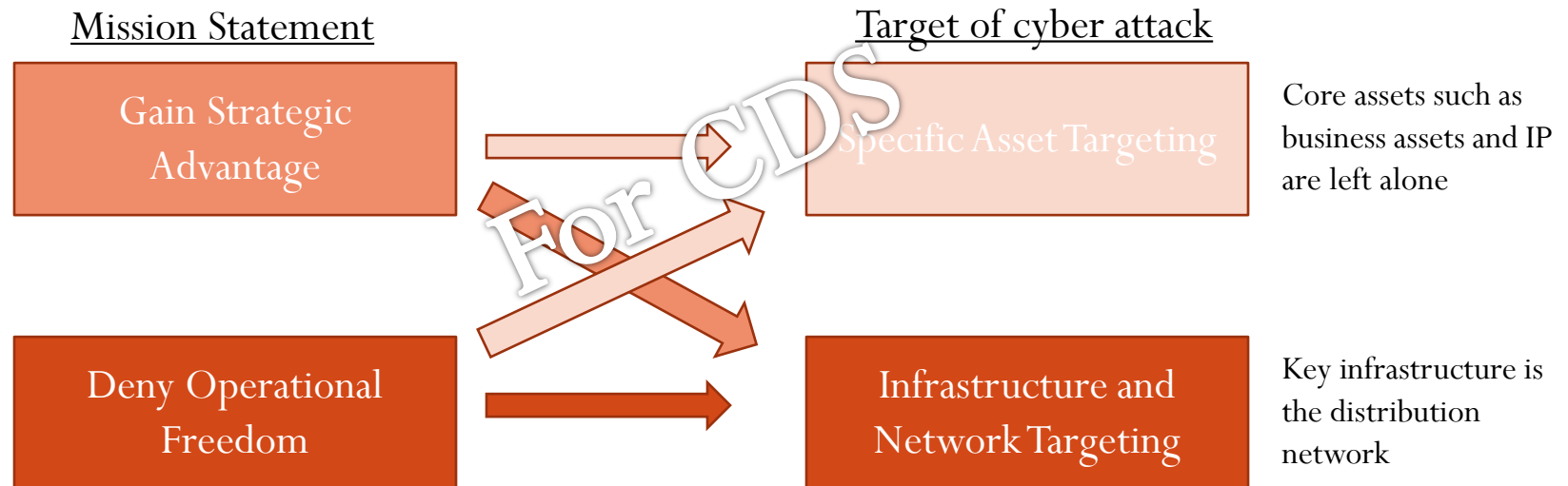
Agriculture & Food	Banking & Finance	Chemical	Dams	Communications	Defense Industrial Base
Energy	Government Facilities	Emergency Services	Healthcare & Public Health	Information Technology	Nuclear Reactors
Postal & Shipping	Transportation	Water	Commercial Facilities	National Monuments	Critical Manufacturing

**Electricity, Petroleum & Natural Gas**

# Attack scenario: defining a mission

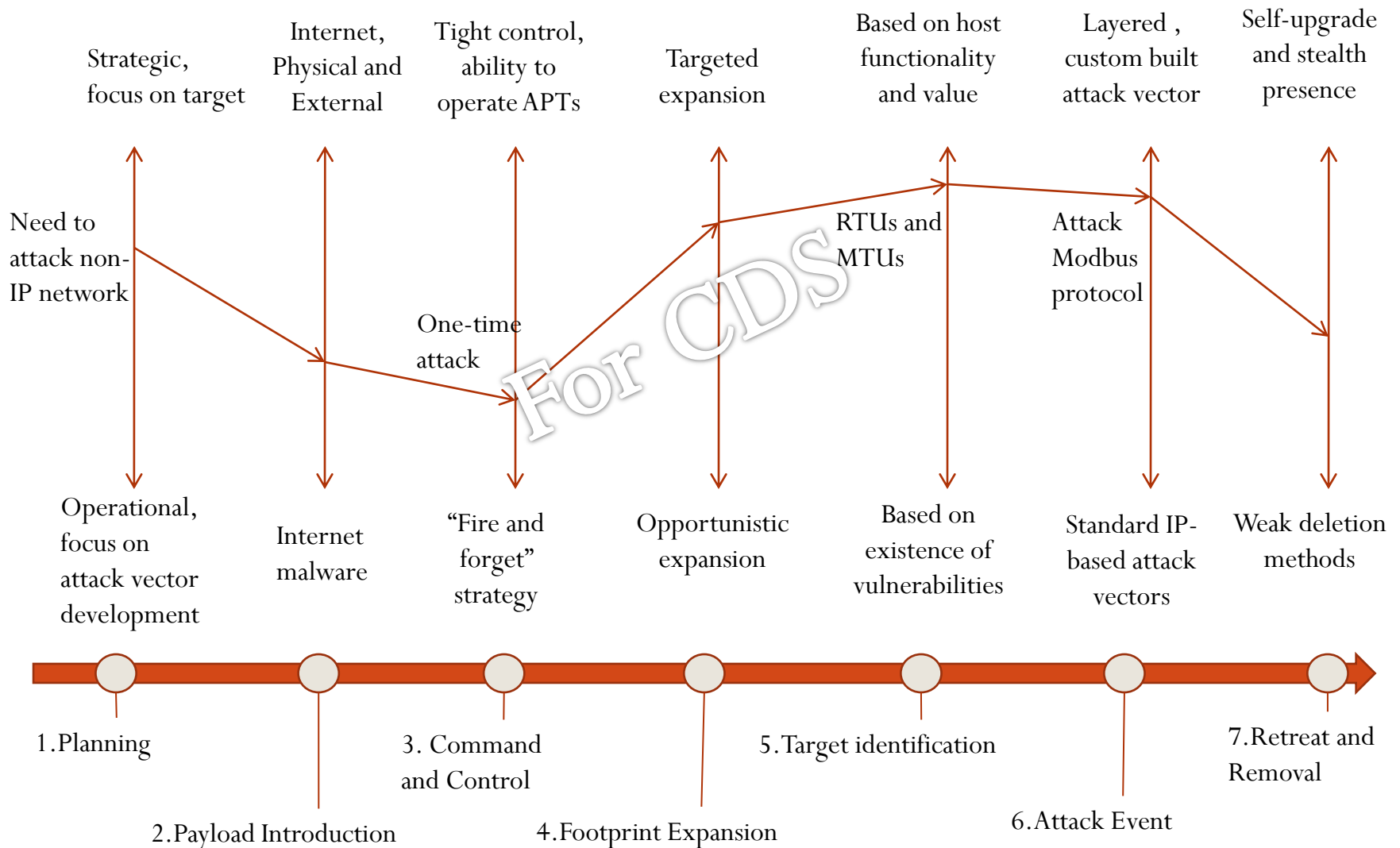
Mission statement: Disrupt a continental US gas pipeline system

Motive: Explore weaknesses, demonstration of power, political statement etc.



Compressor systems represent an attractive infrastructure target

# Attack scenario: identifying cyber attack pathway



# Incidents show that disruptions to oil and gas infrastructure are very costly

- Three week disruption in gas supplies from Russia in 2009 cost Bulgaria cost €250M (\$330M), or 1% of GDP
- Gas plant accident in Western Australia in 2008 cost the region \$6.7B in total
- Terrorist strike on Mexico gas pipelines at Veracruz resulted in \$90-200M in losses
- Shutdown of almost all of French oil refineries in pension strikes in October 2010 cost the French economy up to \$500M per day

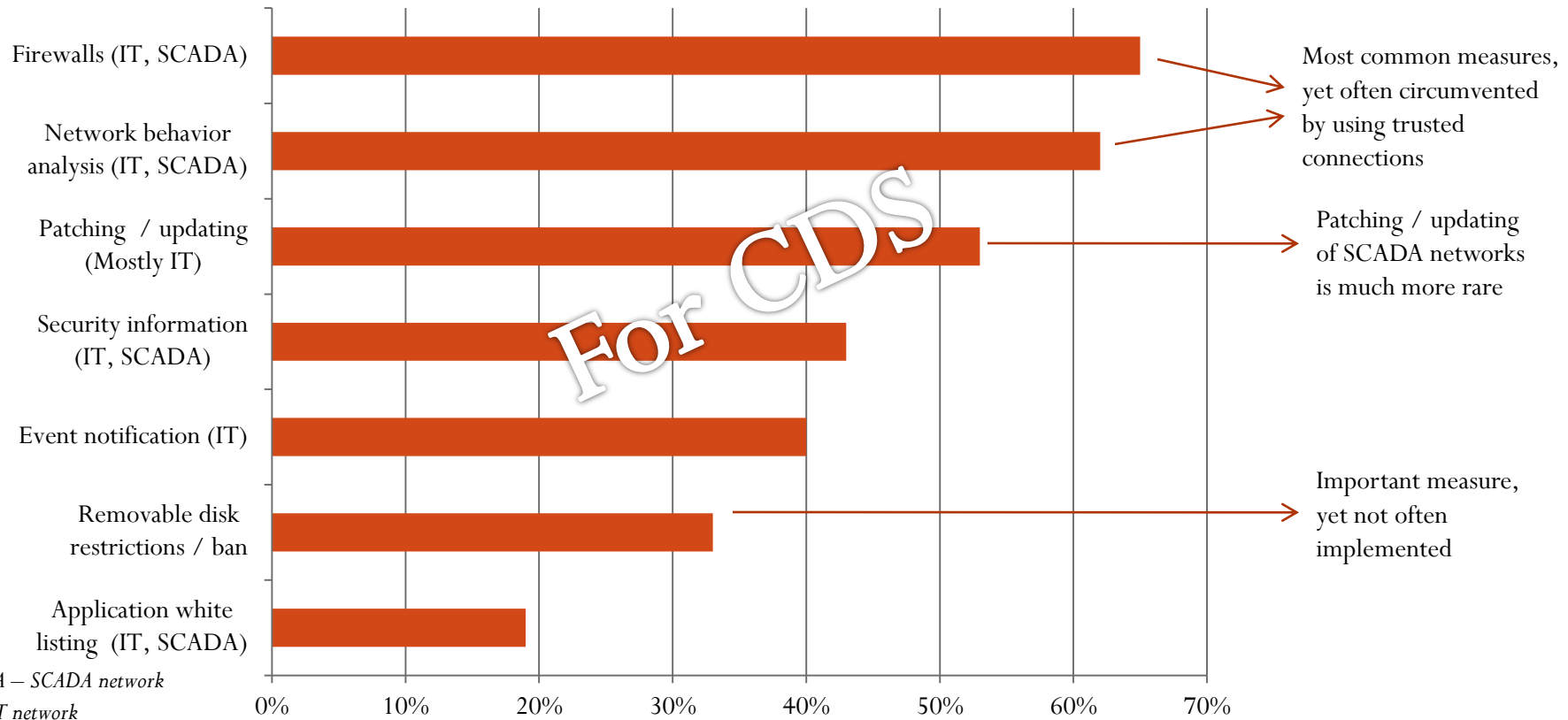
**Losses typically run in millions of dollars per day**

# Agenda

- Cyber Attacks
  - Increasing sophistication of cyber attacks
  - Private Sector as target of, and medium of attacks
- **Vulnerability of the Oil & Gas Industry to Cyber Attacks**
  - Profile of risks faced by SCADA systems in Oil & Gas
  - **Risk Mitigation Strategies and Effectiveness**
- Recommendations

# Risk mitigation by SCADA owners largely based on IT tools

Percentage of companies implementing



**Just perimeter defense is not enough for SCADA networks, what is required is defense-in-depth (defenses embedded in the network)**

# The energy sector has started to respond to the growing cyber threat

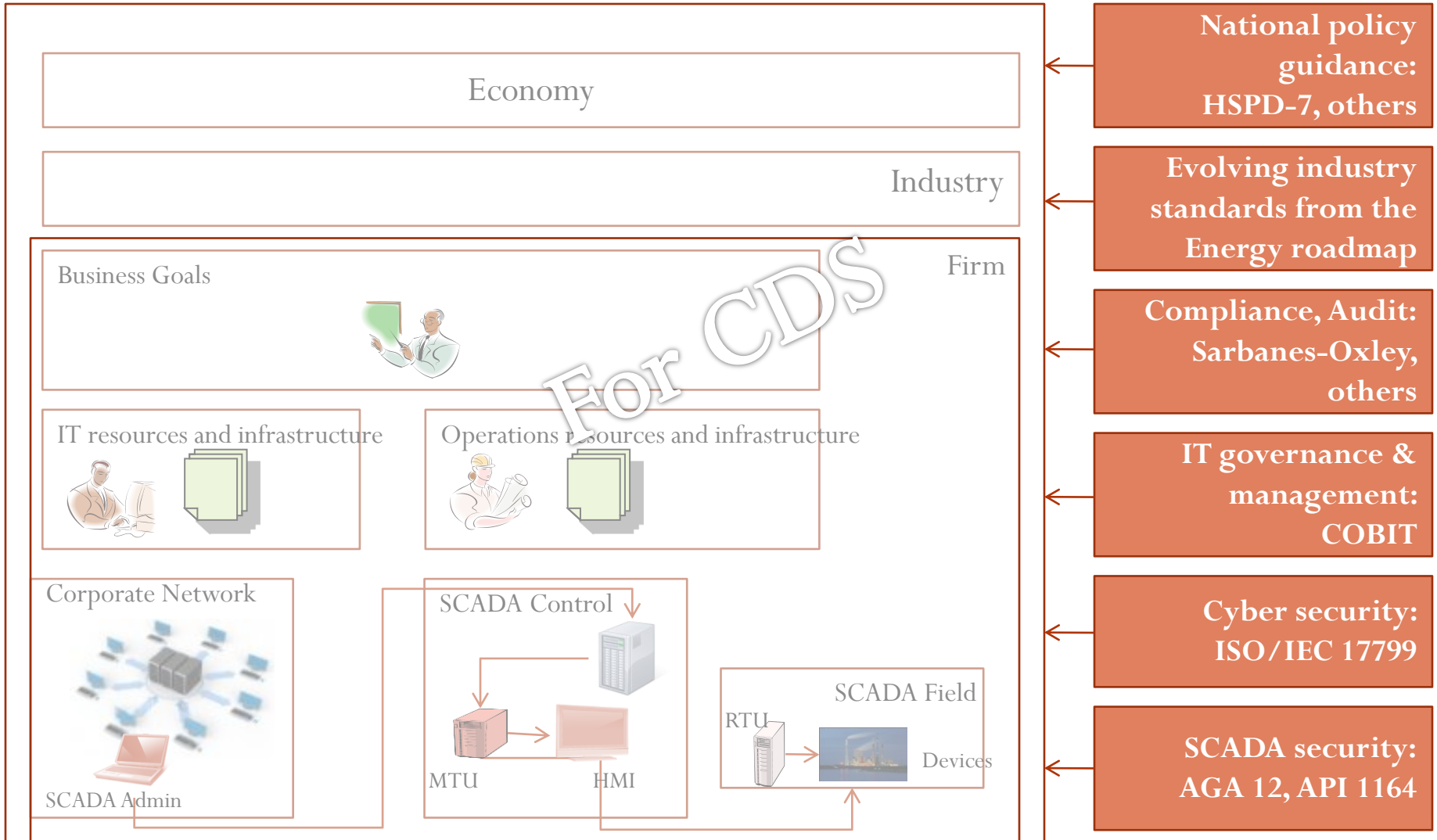
- Is leading to a number of industry initiatives such as the **“Roadmap to Secure Control Systems in the Energy Sector”**
- Initiative between oil & gas, electricity and telecom sector
- 10 year roadmap launched in 2006, and sponsored by DoE and DHS
- Vision: “In 10 years, control systems for critical applications will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function.”
- Participants:
  - Commercial entities – system integrators, component suppliers, technology developers, IT and telecom providers
  - Industry organizations from the oil & gas and electricity sector
  - Research institutes
  - Government agencies
- Successes: More than 100 projects from 21 private and public sector entities under implementation or identified for implementation by 2009

# Security vendors developing frameworks for risk management

## Example of a SCADA risk management framework

- Define critical assets and identify risks
  - Define an electronic security perimeter around process control
    - Main SCADA network + SCADA administration network
  - Manage SCADA assets from behind the perimeter
    - SCADA Administration network should be separate from corporate network
  - Consider the corporate network as untrusted
    - Corporate network should be outside the perimeter
  - Two-factor authentication for any systems outside the perimeter to gain access
    - Will remove the risk of automated attacks, and leave a trail for attacks
- Develop a security policy for critical assets
  - Create policies based on regulations and standards
  - Assess compliance to policies
  - Measure compliance and address deviations from policy

# Policies/standards at various levels play important role in risk mitigation

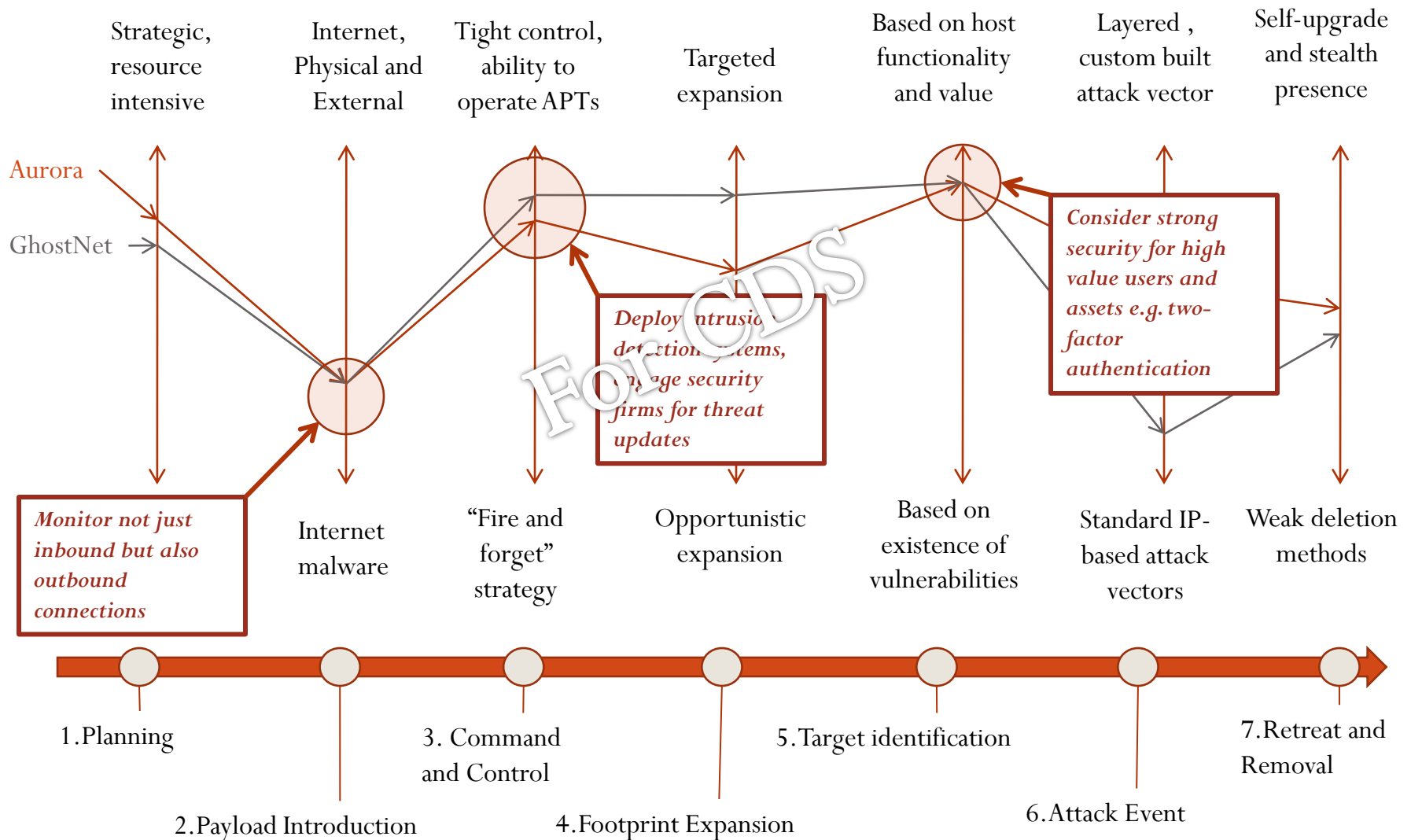


Notes: AGA 12 by the American Gas Association, and API 1164 by American Petroleum Institute

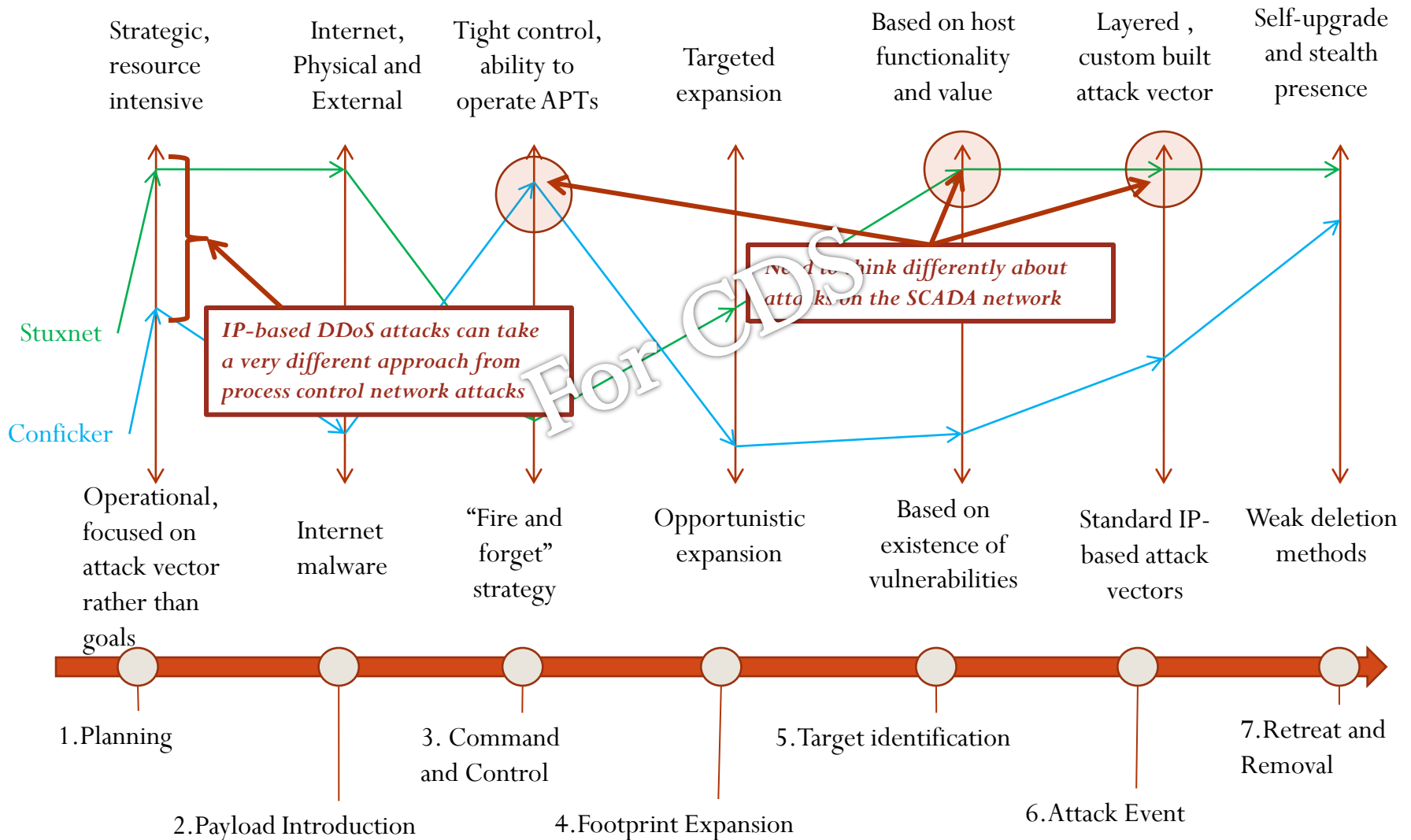
# Agenda

- Cyber Attacks
  - Increasing sophistication of cyber attacks
  - Private Sector as target of, and medium of attacks
- Vulnerability of the Oil & Gas Industry to Cyber Attacks
  - Profile of risks faced by SCADA systems in Oil & Gas
  - Risk Mitigation Strategies and Effectiveness
- **Recommendations**

# Be aware of the common footprints of asset attacks



# However, the footprint of infrastructure attacks may be very diverse



# Selected References / Readings

- *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, for the Executive Office of The President, 2009
- *The command structure of the Aurora Botnet*, Damballa, 2010
- *Natural gas compressor stations on the interstate pipeline network: Developments since 1996*, Energy Information Administration, Office of Oil and Gas, November 2007
- *A Comparison of oil and gas segment cyber security standards*, Idaho National Engineering and Environment Laboratory, November 2004
- *DCS virus infection, investigation and response: A case study*, ICSJWG Fall 2010 Conference
- Berk V., Cybenko G. and Gray R., *Early Detection of Active Internet Worms*, *Massive Computing*, 2005, Volume 5, Part III, 147-180
- *Roadmap to Secure Control Systems in the Energy Sector*, Energetics Inc., January 2006
- *Roadmap Update Workshop Series*, Energy Sector Control Systems Working Group, January 2011
- Haimes Y. and Jiang P., *Leontief-based Model of Risk in Complex Interconnected Infrastructure*, *Journal of Infrastructure Systems*, Vol. 7, No. 1, March 2001, pp. 1-12
- *LOGIIC cyber security system*, Sandia National Laboratories, September 2006
- Haimes Y., Santos J., Crowther K., Henry M., Lian C. and Yan Z., *Risk Analysis in Interdependent Infrastructures*, IFIP International Federation for Information Processing, 2007, Volume 253/2007, 297-310
- *Protecting Your Critical Assets: Lessons learnt from Operation Aurora*, McAfee 2010
- *In the Crossfire: Cyber Infrastructure in the Age of Cyberwar*, McAfee 2010
- *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, for the US China Economic and Security Commission, Northrop Grumman Corporation
- *Cyber Attacks against SCADA and Control Systems*, Byres E. and Paller A., Sans Institute Webinar, 2006
- *W32.Stuxnet Dossier*, Symantec, November 2010
- *State of Enterprise Security 2010*, Symantec, 2010
- David W. Crain, Stan Abraham, (2008), *Using value-chain analysis to discover customers' strategic needs*, *Strategy & Leadership*, Vol. 36 Iss: 4, pp.29 – 39
- *Tracking Ghostnet: Investigating a Cyber Espionage Network*, Information Warfare Monitor, Canada , March 29, 2009

# Selected Web References

- Attack on US oil industry: [http://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved/\(page\)/2](http://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved/(page)/2)
- Attacks on Dept. of Defense: [http://www.businessweek.com/magazine/content/08\\_16/b4080032218430.htm](http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm)
- SCADA basics: <http://www.free-engineering.com/ar-scada.htm>
- Impact of Russia's oil disruption: <http://www.cges.co.uk/resources/articles/2009/08/06/rescuing-russia-europe-gas-relations>
- Impact on Mexico's pipeline incident: [http://www.usatoday.com/news/world/2007-09-10-mexico-pipeline\\_N.htm](http://www.usatoday.com/news/world/2007-09-10-mexico-pipeline_N.htm)
- Cost of French air strikes: <http://www.cbsnews.com/stories/2001/07/25/world/main6991577.shtml>

All images used are the copyright of their respective owners

# About the study

- Independent Study at Tuck School of Business
  - Advisors: Professors Eric Johnson, Brian Tomlin
- Part of the Cyber Code of Conduct project, Fletcher School of Law & Diplomacy
  - Principal Investigator: Professor William Martel

Appendix

For CDS

# Select glossary of terms not explained elsewhere

- IP: Internet Protocol
- Zero-day vulnerability: A vulnerability that is not closed/addressed by developers when a software is released
- Exfiltration: stealth removal of information from target network (in context of cyber attacks)
- DNS: Domain Name System servers, which translate machine names to IP addresses. DNS query refers to querying these servers for machine information. DNS poisoning refers to deliberately introducing translation data to DNS servers
- Active Directory: Windows directory that maintains user names and passwords for a corporate network
- Rootkit: A program that aims to gain root control (right to operate as administrator) without revealing itself
- SQL injection: Subverting/crashing a database-based website by using illegal database queries
- Vishing: Exploiting telephony networks to obtain user information, such as credit card numbers
- Botnets/Zombies: Computers which have been compromised by malware and are used by it to target other computers
- DoS: Denial of Service, refers to crashing a web server by bombarding it with web queries. When this is done by using multiple botnets, it is called distributed DoS (or DDoS)
- Logic bomb: Internet attacks that are set to happen at a particular date or time in the future, or if some condition is met
- Two factor authentication: The requirement of passing two tests before obtaining access. For instance, entering a password and then using a fingerprint before access is given
- VPN: Virtual Private Network
- P2P: Peer-to-peer communication protocol