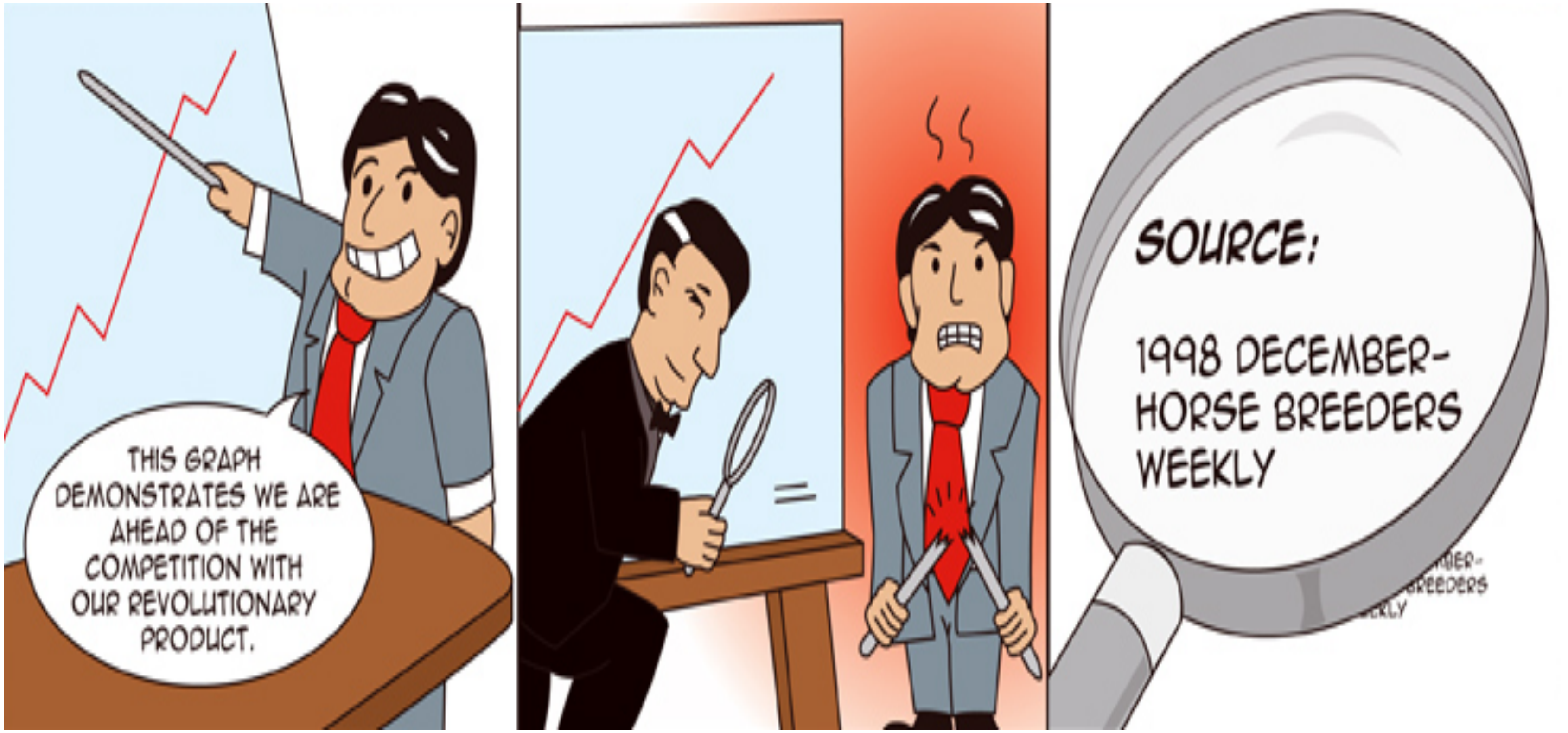
# Cyber Security: The Road Ahead

Dr. Fredrick Mtenzi

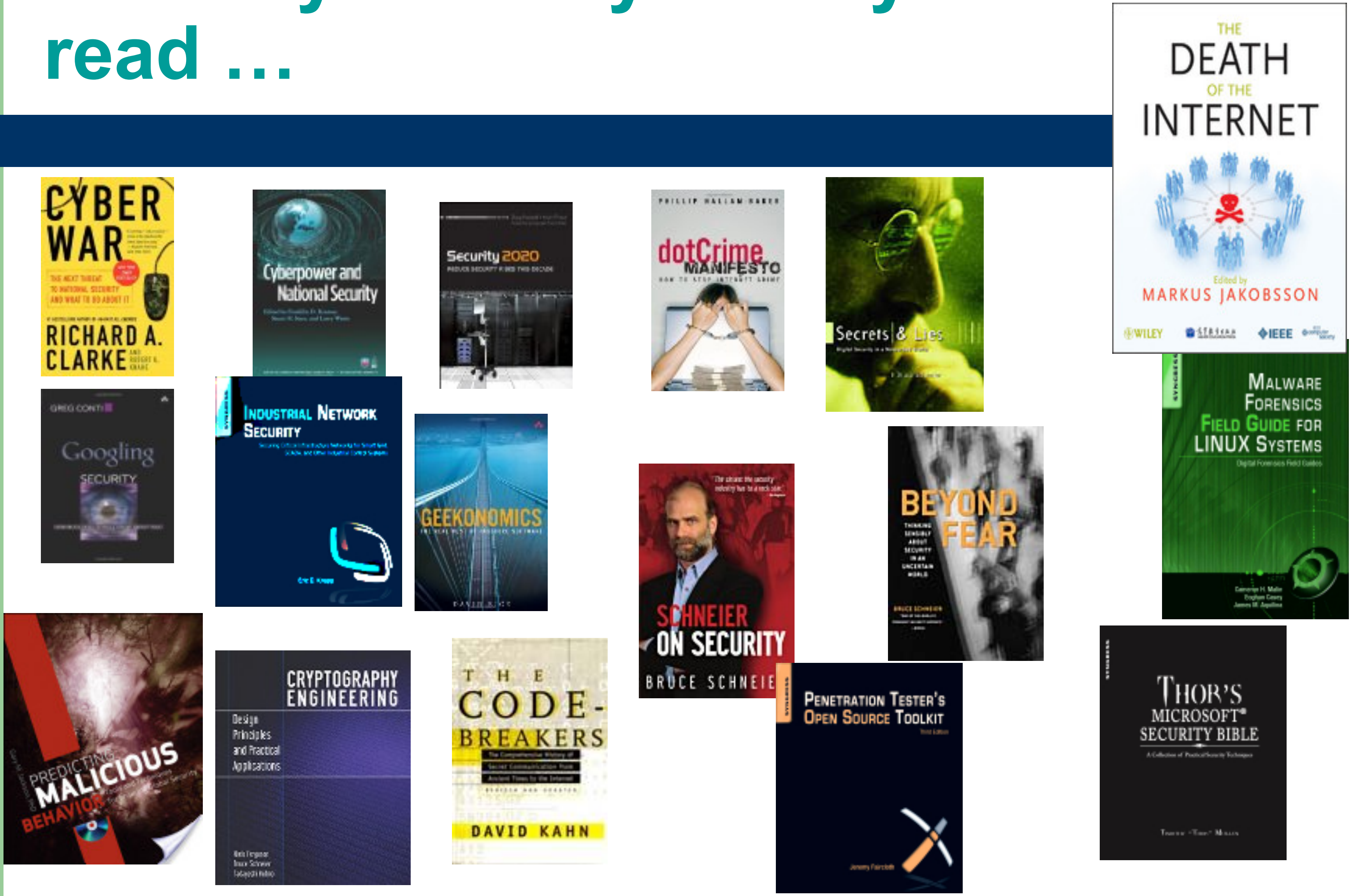
# Agenda

1. Introduction
2. The response
   - The key players
   - Public-Private Cooperation
   - International Cooperating
3. Summary and future work

# Security Statistics


THIS GRAPH DEMONSTRATES WE ARE AHEAD OF THE COMPETITION WITH OUR REVOLUTIONARY PRODUCT.
SOURCE:
1998 DECEMBER-HORSE BREEDERS WEEKLY

# Security Books you may want to read …


CYBER WAR
RICHARD A. CLARKE
Cyberpower and National Security
Security 2020
PHILLIP HALLAM-BAKER
dotCrime MANIFESTO
Secrets & Lies
THE DEATH OF THE INTERNET
MARKUS JAKOBSSON
WILEY
IEEE
GREG CONTI
Googling SECURITY
INDUSTRIAL NETWORK SECURITY
GEEKONOMICS
SCHNEIER ON SECURITY
BRUCE SCHNEIER
BEYOND FEAR
MALWARE FORENSICS FIELD GUIDE FOR LINUX SYSTEMS
PREDICTING MALICIOUS BEHAVIOR
CRYPTOGRAPHY ENGINEERING
Design Principles and Practical Applications
THE CODE-BREAKERS
DAVID KAHN
PENETRATION TESTER'S OPEN SOURCE TOOLKIT
THOR'S MICROSOFT® SECURITY BIBLE

# Web War One (WW1)

- Cyber war is real
- Cyber war happens at the speed of light
- Cyber war is global
- Cyber war skips the battlefield
- Cyber war has begun

*Source: Cyberwar: Richard Clarke and Robert Knake, Harper and Collins Publishers, 2010*

# Web War One (WW1)

- "…May you live in interesting time"

  *Source: Chinese proverb*

- "We cannot solve our problems with the same thinking we used when we created them"

  *Source: Albert Einstein*

# Security 2020

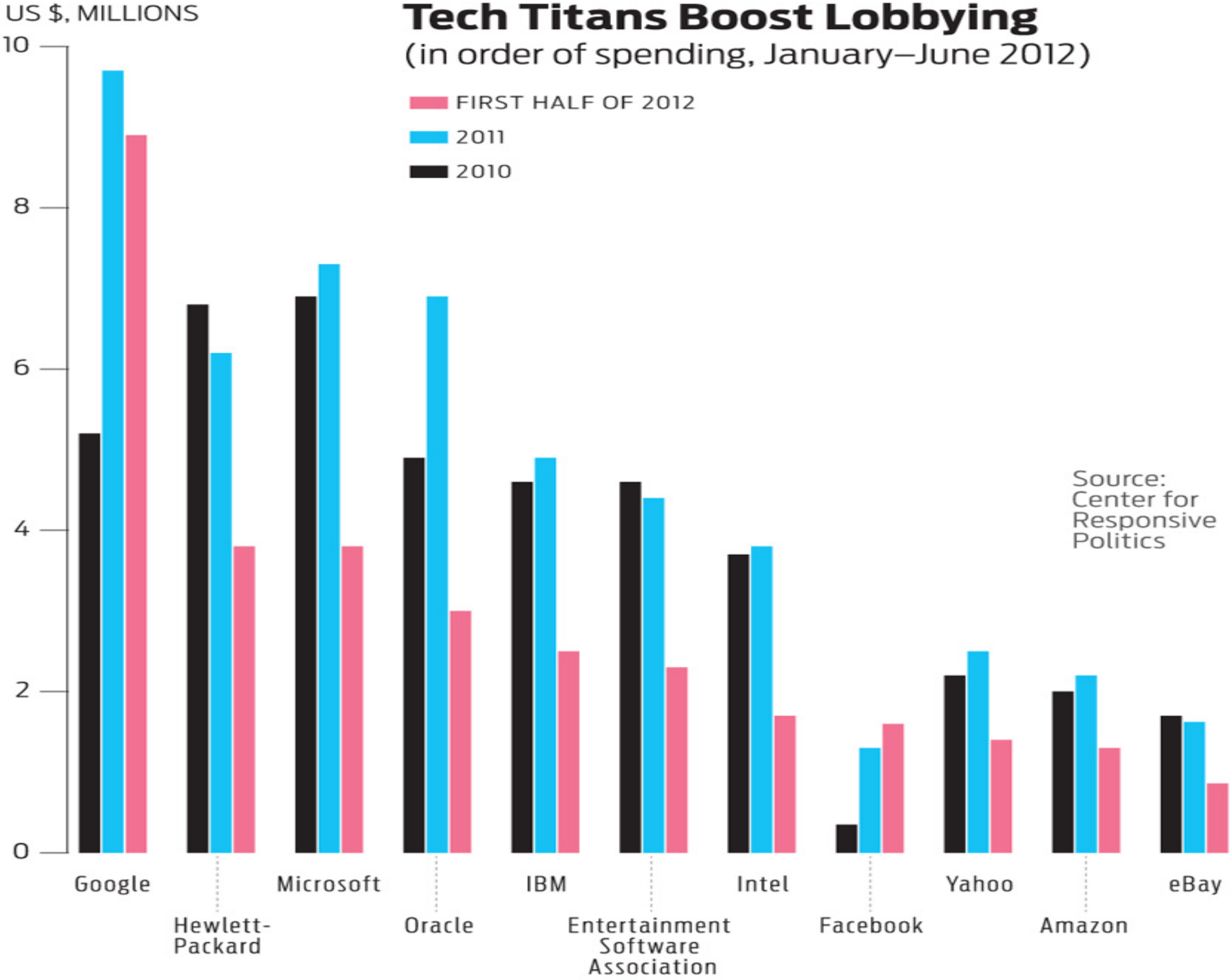
- Consumerization – consumer devices will become trendier, cheaper, and more integrated
- Decentralization – increase use of cloud computing
- Deconcetration – special purpose hardware like iPhone
- Decustomerization – get more IT function without any business relationship: free Google, Bing, Social Networking sites etc

*Source: Security 2020: Reduce Security Risks this decade, Doug Howard and Kevin Prince: Fowarded by security expert Bruce Schneier, 2010*

# Vulnerabilities of the Internet

- The addressing system that finds out where to go on the internet for a specific address – DNS
- The routing among ISPs, a systems known as the Border Gateway Protocol
- Almost everything that makes it work is open, unencrypted
- Its ability to propagate intentionally malicious traffic designed to attack computers
- It is one big network with a decentralised design

*Source: Cyberwar: Richard Clarke and Robert Knake, Harper and Collins Publishers, 2010*

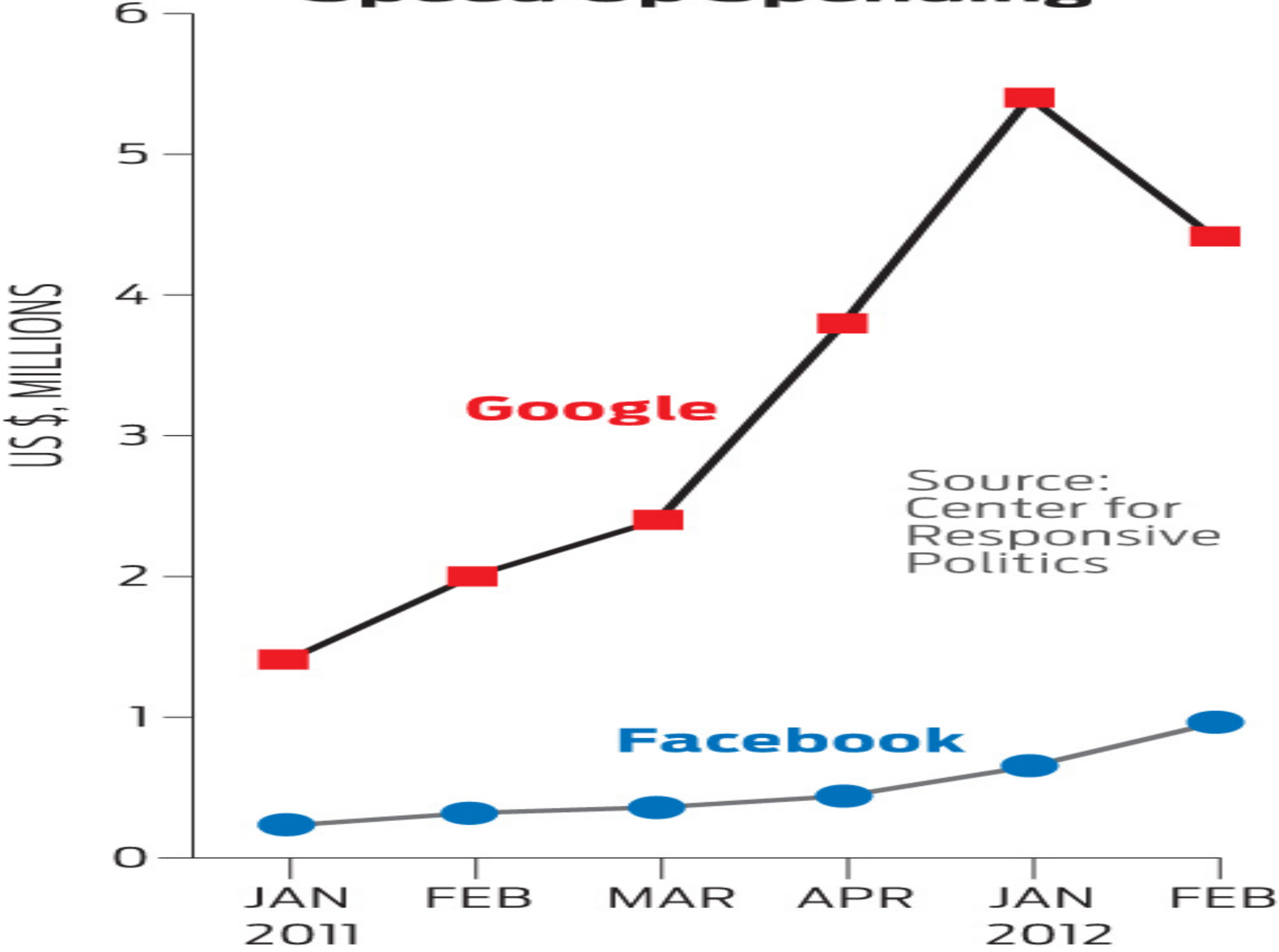


# Tech Titans Boost Lobbying

(in order of spending, January–June 2012)

Source: Center for Responsive Politics

## Google and Facebook Speed Up Spending



Source:
Center for
Responsive
Politics

# Cyber Security

- Cyber security encompasses borderless challenges
- Our response have remained overwhelmingly national in scope and this is insufficient
- There are enormous gaps in our understanding of Cyber security, as well as in the technical and governance capability to confront it
- Democratic governance concerns particularly control, oversight and transparency have been absent from the debate

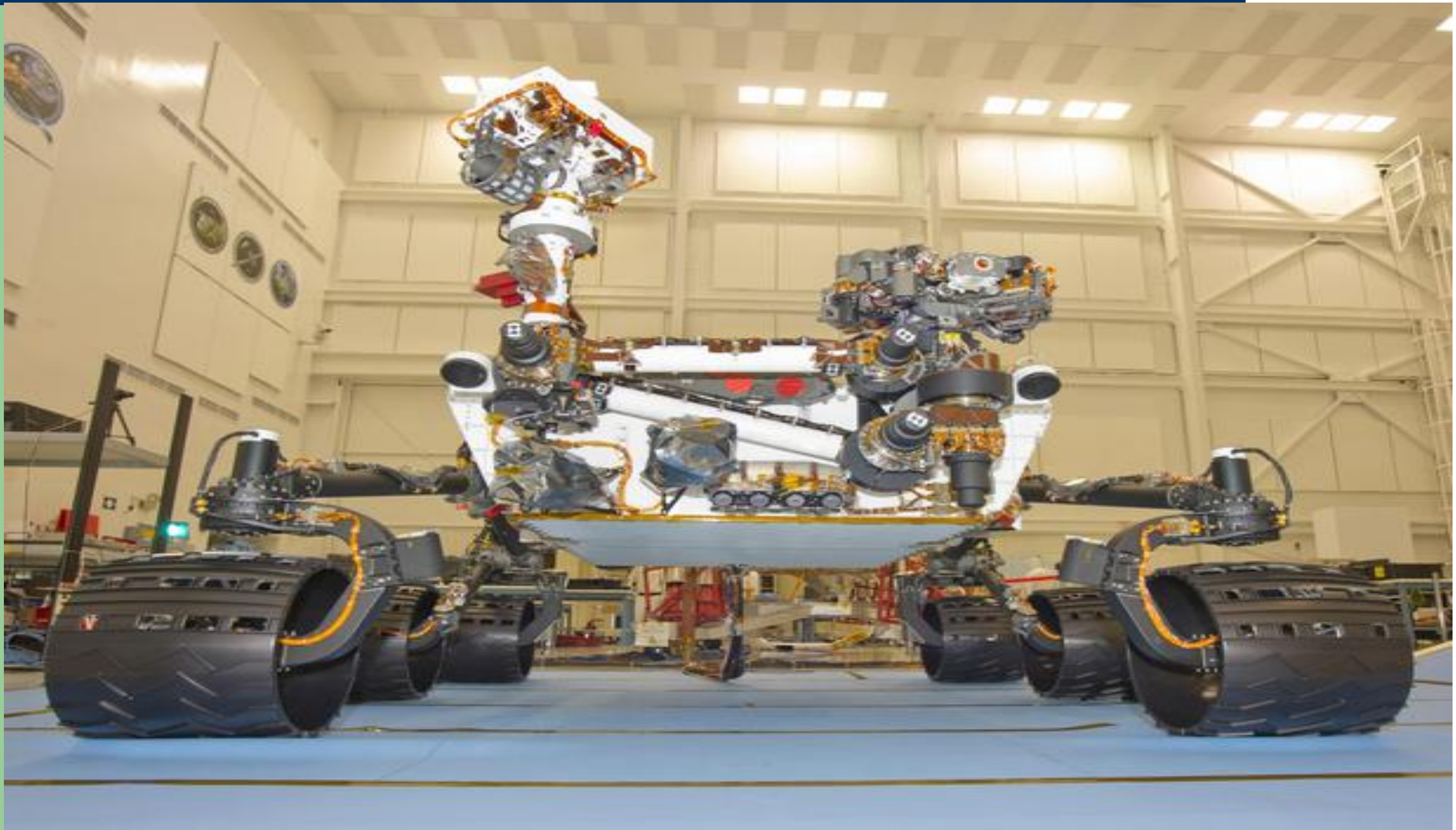
# Cyber Security

- Cyberspace is defined by its ubiquitous connectivity. However, that same connectivity opens cyberspace to the greatest risks
- As the networks increase in size, reach and function, their growth equally empowers law-abiding and hostile actors
- Seemingly localised disruptions can cascade and magnify rapidly, threaten other entities and create systemic risk

# Cyberspace

- Cyberspace, the 5th space of warfare (after land, sea, air, and space) consists of all of the computer networks in the world and everything they connect and control via cable, fibre-optics or wireless
- Cyberspace includes the Internet plus many other networks of computers, including those that are not supposed to be accessible from the internet

# Next Generation Mars Science Laboratory rover



# The Issues: Cyberspace

- Cyber criminals can hack into networks and controls or crash them. Examples of damage range from stealing information to compromising critical systems such as the electric power grid.
- Thus a loss of power of just a few days could produce a cascade of economic damage as money runs out and food becomes scarce

# The Issues: Cyberspace

- Mission critical systems can be exploited or attacked from remote locations
- These attacks are possible because of flaws in the design of the internet; flaws in hardware and software; the move to put ever more critical systems online; the lack of effective deterrents; and absence of appropriate defence mechanisms
- Threats in cyberspace are as broad and diverse as cyberspace itself

# The Issues: Cyberspace

- It is increasingly cheap to launch destructive cyber attacks anonymously, but ever more expensive to defend against such attacks
- This growing asymmetry is the real game changer
- The modern thief can steal more money with a computer than with a gun
- Tomorrow’s terrorist may be able to do more damage with a computer keyboard than with a bomb

# Cyber crime

- Cyber crime is a clear and present danger that has turned into a silent global digital epidemic
- Cyber crime encompasses a wide range of offences, including hacking of computers, data and systems, computer related forgery and fraud such as phishing and pharming and copyright offences via dissemination of pirated content

# Cyber crime

- Current defensive, prevention and protection techniques are providing little defence and are rapidly becoming obsolete
- Cyber criminals are leveraging innovation at a pace which many governments, organisations and security vendors can no longer match
- Malware authors and cyber criminals now provide skills, capabilities, products and outsource services to other cyber criminals

# Cyber crime

- The cyberspace offers to criminals anonymity and the ability to allow otherwise un-associated individuals in different parts of the world to network on a transactional basis
- Organised cyber criminals are working in swarms (http://www.gartner.com/it/page.jsp?id=1416513)

# Why Cyber crime will increase in the future?

- The technology of cyber crime has become more accessible
- The profile of the internet users is changing
- Offenders can now increase the number of attacks exponentially through use of automation and growing bandwidth

# Trends in cyber crime demand a much more serious response

- Cyber crime attacks and security breaches will increase in frequency, complexity and sophistication, with discovery occurring after the fact, if at all
- Most indicators point to future cyber crime attacks becoming more severe, more complex, and more difficult to prevent, detect, and address

# Trends in cyber crime demand a much more serious response

- Effective deterrents to cyber crime are not known, not available or not accessible to a majority of practitioners, many of whom still underestimate the scope and severity of the problem
- Lack of accurate intrusion reporting to regulators and law enforcement is the core reason that issues related to cyber security and cyber crime are not being recognised as the most immediate priority

# The strategic challenges

- The threats to cyber security are the greatest national and economic security threats countries face. Yet remains least understood and most underestimated threat
- The very complexity of the threat deters a full understanding of its implications and hinders a comprehensive debate on the strategic responses needed
- Cyber security is a cross-cutting issue that permeates all aspects of life of a modern society and economy. This makes identification and solutions procedures more difficult

# The strategic challenges

- The ability to misuse, manipulate, or even dominate cyberspace will increasingly attract organised crime
- Cyberspace needs to be understood increasingly as the most important theatre of military operations – Cyberwar and Cyber dominance
- The omnipresence of cyber issues in modern life will require not only military answers to the threat, but a fully integrated strategy by the entire security sector

# The strategic challenges

- Cybersecurity cannot be achieved at the nation state alone. It requires partnership, collaboration and cooperation from everyone
- If the problems posed by cybersecurity cannot be solved, the implications will be severe. There is a genuine risk that the internet will become dysfunctional or disintegrate into a set of separate intranets

# Why we have not acted to solve Cybersecurity problems?

- A lack of proper incentives (or liability) for technology and software producers to integrate security elements
- An unrealistic expectation that the end-user is able, willing or aware enough to be responsible for security in all guises
- Divergent legal systems and laws relating to cyber crime and cyber security in the world
- Virtually no consequences/sanctions for cybercriminals due to inherent difficulties in implementing legal procedures within and outside national borders

# Why we have not acted to solve Cybersecurity problems?

- The inability of some governments to cooperate fully due to national security priorities
- The lack of reporting and monitoring of cybercrimes, malware and fraud online
- The challenge for developing countries to finance necessary cybersecurity measures; without which the global system remains highly insecure
- A lack of trained personnel

# Key Players: Government

- Must establish Cyber Security Strategy
- Encourage international collaboration and work to reduce the “Cyber Abyss” between developed and developing countries
- Must provide leadership, legal framework, organisation stability and expertise in cyber security related issues

# Key Players: Legislative Bodies

- The technical complexity of cyber security in most cases surpasses the knowledge and experience of members of the parliament
- Cyber security is cross-cutting issue makes it hard to decide which committee is in charge in the parliament
- How to measure performance in cyber security issues is hard, in the absence of best practices from other implementation

# Key Players: Legislative Bodies

- In most countries cyber security issues are headed by the military or intelligence agencies making transparency hard to achieve
- There is no clear definition of what constitutes a cyber attack and therefore, legislative bodies cannot decide when the country is at cyber war. The anonymity of attackers and countries not being willing to be responsible of the actions of their citizens does not help

# Key Players: Armed Forces

- The military has become completely dependent on cyberspace, any threat in the cyber domain is of fundamental consequence
- Use of high tech equipment has rendered the military vulnerable to cyber attacks
- The inertia of the military to embrace new technologies – “the military always tends to prepare for the last war”
- There are few examples of cyber power in action such as Estonia, Georgia and “Stuxnet” attack on Iran. Others are Duqu, Flame and Shamoun

# Key Players: Armed Forces

- Stuxnet is weaponised software that target industrial control systems -> cyber war
- Cyber defence on large scale requires cooperation between private sector and the military
- If cyber replaces kinetic as prime manifestation of prime power the changes in the military will be phenomenal

# Key Players: Armed Forces

- Cyber advances will have a serious impact on the relative military strength of nations and the international balance of power
- Cyberspace presents the military with questions for which there are not only no answers, but for which we might not even have understood the questions yet

# Key Players: Law Enforcement

- Perpetrators and victims are frequently located in different jurisdictions posing acute difficulties for law enforcement investigating and prosecuting online crimes
- The speed at which cyber criminals can inflict harm and evade detection puts law enforcement under heavy pressure, making the need for international cooperation more pressing

# Key Players: Law Enforcement

- Law enforcement lack expertise, responsiveness, techniques and procedures for responding to cybercrimes, insufficient cyber forensics personnel and outdated or nonexistent legal remedies
- The response to criminal activity in physical world is hard to replicate in cyberspace

# Key Players: Judges and Prosecutors

- All judges, investigative judges and prosecutors should have basic knowledge of matters related to cyber crime and electronic evidence
- Cyber crime laws are not update, contain loopholes or do not exist at all, penalties for cyber crime are weak; many impediments exist for investigators in forensics search and seizure and in obtaining witness cooperation

# Key Players: End User

- User must be aware of the risks of cyber crime, as well as the best practices required to protect themselves
- The public must become aware that attack on CNI can cause loss of life, threaten public safety, impact national security, cause widespread economic upheaval, or create environmental disasters
- Public must be aware of the importance of reporting all electronic intrusions and associated losses to law enforcement

ORACLE

Google

amazon.com

# Key Players: Private Sector

- The private sector response to cyber security can be characterized as unstructured
- There are three responses to market failures of this sort: regulation, taxation and insurance pricing
- The relevant insurance question is: how to underwrite the risk? And the answer only can come if the risk-taker is motivated by liability to insure the risk in the first place

# Key Players: Private Sector

- It is not easy for the government to propose regulatory mandates in a complex technical area like cyber security
- Taxing remains a tool by which governments have frequently sought to modify private actor conduct
- Can the private sector police itself in cyber security?

# Key Players: IT sector

- The IT sector is a critical part of any cyber security solution
- The quality of software needs to improve
- The security attention is moving from OS to the application layer and the lower level such as firmware are poised to be next target of attack
- Relying on the end-user to be responsible for the security of her PC or devices is perhaps akin to asking a driver to purchase her own seatbelt or airbag

# Key Players: Banks and Financial Services

- IT investment in online banking, brokerage and insurance services has focused to increase convenience, improve QoS and reduce cost
- These benefits bring new and virulent risks of fraud, theft, extortion, credit quality deterioration as well as systemic risk

# Key Players: Banks and Financial Services

- Reasons why banks or financial services do not report intrusions or losses include:
  - Negative publicity
  - Negative information competitors would use to their advantage
  - The need to protect individual customer's privacy
  - The risk of exposing themselves to costly and time consuming litigation
  - Fear among IT personnel of reporting incidents due to worries about job security
  - Lack of trust towards law enforcement, or concern that reporting may lead to increased regulation of the industry or of e-commerce in general

# Key Players: Critical National Infrastructure

- Every sector of private and public life is a potential target for criminal cyber attacks – for covert probing, intelligence gathering or sabotage operations by foreign powers
- The process of protecting CNI requires a high degree of cooperation and information sharing among key players being led by the government

# Key Players: WikiLeaks

- WikiLeaks has published classified documents in spectacular fashion
- This is an internet platform dedicated to the disclosure of private/classified information and open to all
- WikiLeaks is a highly commercial enterprise – relationship with Spiegel.online and The New York Times

# Key Players: WikiLeaks

- WikiLeaks posses more questions:
  - The right of the public to know vs the right to privacy
  - How to protect governments from massive leaks through disgruntled personnel?
  - How to protect at the private level (from Facebook to Smartphone) –confidential, personal and private data?
  - How to handle the issue in the integrated fashion at the national level?
  - What international action is needed and appropriate?
  - If answers are not found urgently, the anarchic reaction to the WikiLeaks drama will transform itself into a permanent and dangerous phenomenon

# The response: Public-Private Partnerships

- The private sector is reluctant to share sensitive proprietary information with government or its competitors because of risky and less than clear benefits
- They fear that sharing information with government may lead to increased regulation
- There is a general lack to trust towards law enforcement and private sector fear being caught in investigations and lose production

# The response: Public-Private Partnerships

- There is a prospect that confidential information shared may be disclosed using acts such as Freedom of Information Act
- There is strong sharing culture among private sector without intervention from the government such as white-hate hacker and security research community

# Unique attributes to cyber security partnership

- Issues of property in the cyber realm, both intellectual and in asset valuation
- Traditional PPC operates under established regulatory structures, such structures do not exist in the cyber domain
- The time scale involved in cyber development, incident, response and threat indications are shorter than in traditional PPC

# Essential capabilities for the cyber security partnership to be successful

- Detection: the partnership must define, identify and watch for behaviour concerns
- Protection: it must ensure compliance with partnership's security standards, sanctioning those who fail to comply
- Response: which must provide a means to conduct forensic examinations following disruptions, analyse vulnerabilities and effectively attribute attacks to their perpetrators

# Essential capabilities for the cyber security partnership to be successful

- Inspection and enforcement of standards upon suppliers and ISPs
- The ability to watch networks, search for and analyse future threats, and warn all users before and emergence occurs
- The ability to respond to attacks, through warnings and technical fixes, as well as to plan for the recovery of crucial systems after an emergence

# Essential capabilities for the cyber security partnership to be successful

- Necessary protection of privacy and free speech, individual rights and business concerns, cognizant of government needs
- Mechanisms for international collaboration on cyber security

# The Response: International Cooperation

- There are several regional and international cyber security initiatives such as:
  - Council of Europe’s Convention on Cyber Crime
  - European Network and Information Security Agency (ENISA)
- Protecting cyberspace and the digital infrastructure is a shared responsibility of government, private sector, international organisations and users

# Important Cyber Security Questions

- How will we define what constitutes a cyber-attack and what kind of retaliation is realistic, effective and appropriate?
- Does this mean that we will have to stay one step ahead of the attacker with constantly evolving and innovative software and hardware? Is this realistic?
- How can government and/or militaries hope to be quicker, faster and more agile than the cyber enemy?
- Are countries already de-facto in the process of abdicating their responsibility for security of citizens and key business sectors to private cyber-security firms? How can the trend be reversed?

# Important Cyber Security Questions

- There is a clear move to fragment the cyberspace for several reasons such as national boundaries and censorship, language etc. Are we moving into an age of internet protectionism? What will this mean?
- What about privacy and identity in an age of heightened cyber security? How will increased focus on cyber security affect the web as we know it today? Will cyber security take precedence over freedom?

# Important Cyber Security Questions

- What are the peripheral uses of new technology designed specifically for defence purposes? Have we given enough thought to it? What about its potential use for employers, marketing agencies and others to monitor individuals' behaviour at work and online? Will privacy exist in the future?

# Important Cyber Security Questions

- If there is a cyber gap between the US and EU and cyber abyss between the OECD and the developing world, how can cyber failed states be prevented and the South's ability be improved to meet the security, regulatory, and technical challenges of online security?
- How can states detect and respond to the emerging threat of cyber war? Clearly, new forms of private public cooperation are needed. But what forms should they take, how transparent should they be, and how can they be best subjected to parliamentary and democratic control?

# Important Cyber Security Questions

- What is the responsibility of states regarding attacks by groups and individuals operating on their territory?
- How can regulation deal with the international nature of the threat? What international approaches and norms are conceivable and needed? Who should take the lead in this issue?
- How to shape, in an open debate, national consensus, strategies, and policy in this area?
- Is time on our side? Or is technological change outpacing regulatory efforts and the drive for democratic control?

# Important Cyber Security Questions

- Is cyber war replacing kinetic energy as the core essence of military power? Are we witnessing a second wave of the revolution in military affairs? Is the face of battle to be changed fundamentally? If so, what will be the implications for the armed forces and the security at large? What will be the implications for intelligence services? For law enforcement agencies?

# Proposed measures needed for discovering and monitoring cyber threats and risks

- Establishing real-time surveillance, monitoring, and early warning capability of attacks, and a capability for sharing critical response information with key stakeholders
- Implementing intrusion detection systems using passive sensors to identify when unauthorized users attempt to gain access to networks and IT systems
- Strategically addressing identity management, authentication, credential and access management to provide assurance that critical systems are accessed by authorised individuals

# Proposed measures needed for discovering and monitoring cyber threats and risks

- Developing malicious code detection methods that go beyond simple signature detection for long term detection and analysis
- Developing methods for determining the source of malicious behaviour through analysis of network topology and traffic that also work in the presence of IP spoofing
- Developing online learning methods for dynamic modelling, for modelling data with skewed class distributions, and feature selection for data with evolving characteristics

# Proposed measures needed for countering cyber threats and risks

- Achieving a more reliable, resilient and trustworthy digital infrastructure for the future
- Developing a cyber security strategy, designed to shape the international environment on issues such as technical standards, acceptable norms, sovereign responsibility and use of force
- Carrying out comprehensive assessments of the vulnerabilities of key resources and critical infrastructure, including risk assessments to determine risk posed by particular types of attacks
- Developing a comprehensive national plan to deal with these vulnerabilities.

# Proposed measures needed for countering cyber threats and risks

- Better defining roles, lead-responsibility and accountability of government entities in securing critical national infrastructures, government networks, and IT systems
- Making concerted and collaborative research development in cyber and critical infrastructure security a national priority
- Establishing working groups charged with conducting annual reviews of research and development initiatives in their sectors, and recommending updates to the priorities based on changes in technology, threats, vulnerabilities, and risk

# Proposed measures needed for countering cyber threats and risks

- Encouraging the private sector to perform periodic vulnerability assessments of CNI
- Conducting performance audits in accordance with generally accepted government auditing standards
- Establishing effective coordination and information sharing between public and private sector participants in response to significant cyber incidents

# Proposed measures needed to solve the legal challenges

- Establishing, reviewing, and modernizing criminal law, procedures for electronic investigations, and policy to ensure the capability exist to prevent, deter, respond to, and prosecute cybercrime
- Establishing dedicated cyber crime units, electronic forensics, training, and outreach for all who have a role in organising a unified response to cyber incidents and deterring cybercrime, including the judiciary and the private sector

# Proposed measures needed to solve the legal challenges

- Establishing, reviewing, and updating legal infrastructures related to data protection, privacy, digital signatures, commercial law, e-government, and encryption in close consultation with experts across government and civil society
- Reconciling differing national laws concerning investigation and prosecution of cybercrimes, data protection, preservation, and privacy, and addressing the problem of existing cyber laws of other countries that do not carry enforcement provisions

# Proposed measures needed to create a skilled cyber workforce and public awareness to promote cyber security

- Overcoming the major challenges in attracting, hiring, training, retaining, and effectively managing cyber security and forensics talent, and introducing more attractive career tracks
- Reaching agreement on the scope of educational efforts and projects to ensure that adequate cadre of skilled personnel is developed to protect IT systems and redirecting efforts to build a professional cyber workforce for now and future needs

# Proposed measures needed to create a skilled cyber workforce and public awareness to promote cyber security

- Initiating national public awareness and educational campaign to promote cyber security, to expand support for key education programs, and research and development to ensure the nation’s continued ability to compete in the information age economy

# The keys for creating an effective Cyber Security Strategy

- Develop a cyber security strategy that clearly articulates strategic objectives, goals and priorities
- Establish top-level government responsibility and accountability for leading and overseeing the national cyber security policy
- Establish a governance structure for the strategic implementation of cyber security strategy
- Publicize and raise awareness about the seriousness of the cyber security problem
- Create an accountable, operational cyber security organisation leading the implementation

# The keys for creating an effective Cyber Security Strategy

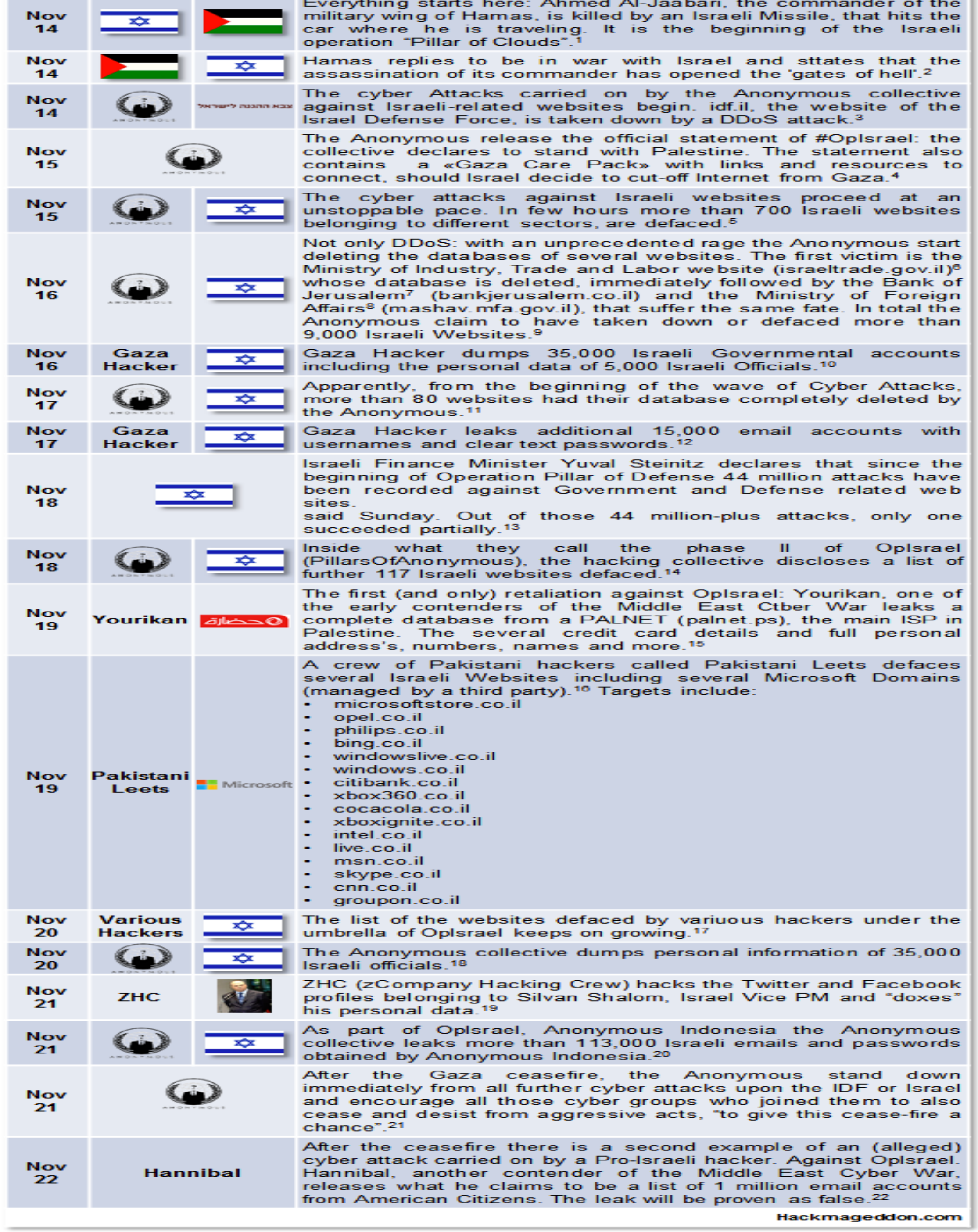
- Bolster public private partnerships through an improved value proposition and use of more incentives
- Focus much greater attention on addressing the global aspects of cyberspace
- Improve law enforcement efforts on addressing malicious activities in cyberspace

# The keys for creating an effective Cyber Security Strategy

- Place greater emphasis on cyber security research and development, including consideration of how to better coordinate government and private sector efforts
- Increase the cadre of cyber security and forensics professionals
- Make the government a model for cyber and CNI security, including using its acquisition function to enhance cyber security aspects of products and services

# Cyber security

- Many security programs are based on reactive measures such as software patching, instead of proactive measures that prevent attacks in the first place
- Will the internet be there when you really need it?
- We are too dependent on the internet and are underestimating risks for the sake of cost, convenience and efficiency



| | | | |
|---|---|---|---|
| Nov 14 | 🇮🇱 | 🇵🇸 | Everything starts here: Ahmed Al-Jaabari, the commander of the military wing of Hamas, is killed by an Israeli Missile, that hits the car where he is traveling. It is the beginning of the Israeli operation "Pillar of Clouds".[1] |
| Nov 14 | 🇵🇸 | 🇮🇱 | Hamas replies to be in war with Israel and sttates that the assassination of its commander has opened the 'gates of hell'.[2] |
| Nov 14 | ANONYMOUS | צבא ההגנה לישראל | The cyber Attacks carried on by the Anonymous collective against Israeli-related websites begin. idf.il, the website of the Israel Defense Force, is taken down by a DDoS attack.[3] |
| Nov 15 | ANONYMOUS | | The Anonymous release the official statement of #OpIsrael: the collective declares to stand with Palestine. The statement also contains a «Gaza Care Pack» with links and resources to connect, should Israel decide to cut-off Internet from Gaza.[4] |
| Nov 15 | ANONYMOUS | 🇮🇱 | The cyber attacks against Israeli websites proceed at an unstoppable pace. In few hours more than 700 Israeli websites belonging to different sectors, are defaced.[5] |
| Nov 16 | ANONYMOUS | 🇮🇱 | Not only DDoS: with an unprecedented rage the Anonymous start deleting the databases of several websites. The first victim is the Ministry of Industry, Trade and Labor website (israeltrade.gov.il)[6] whose database is deleted, immediately followed by the Bank of Jerusalem[7] (bankjerusalem.co.il) and the Ministry of Foreign Affairs[8] (mashav.mfa.gov.il), that suffer the same fate. In total the Anonymous claim to have taken down or defaced more than 9,000 Israeli Websites.[9] |
| Nov 16 | Gaza Hacker | 🇮🇱 | Gaza Hacker dumps 35,000 Israeli Governmental accounts including the personal data of 5,000 Israeli Officials.[10] |
| Nov 17 | ANONYMOUS | 🇮🇱 | Apparently, from the beginning of the wave of Cyber Attacks, more than 80 websites had their database completely deleted by the Anonymous.[11] |
| Nov 17 | Gaza Hacker | 🇮🇱 | Gaza Hacker leaks additional 15,000 email accounts with usernames and clear text passwords.[12] |
| Nov 18 | 🇮🇱 | | Israeli Finance Minister Yuval Steinitz declares that since the beginning of Operation Pillar of Defense 44 million attacks have been recorded against Government and Defense related web sites.<br>said Sunday. Out of those 44 million-plus attacks, only one succeeded partially.[13] |
| Nov 18 | ANONYMOUS | 🇮🇱 | Inside what they call the phase II of OpIsrael (PillarsOfAnonymous), the hacking collective discloses a list of further 117 Israeli websites defaced.[14] |
| Nov 19 | Yourikan | حضارة | The first (and only) retaliation against OpIsrael: Yourikan, one of the early contenders of the Middle East Ctber War leaks a complete database from a PALNET (palnet.ps), the main ISP in Palestine. The several credit card details and full personal address's, numbers, names and more.[15] |
| Nov 19 | Pakistani Leets | Microsoft | A crew of Pakistani hackers called Pakistani Leets defaces several Israeli Websites including several Microsoft Domains (managed by a third party).[16] Targets include:<br>- microsoftstore.co.il<br>- opel.co.il<br>- philips.co.il<br>- bing.co.il<br>- windowslive.co.il<br>- windows.co.il<br>- citibank.co.il<br>- xbox360.co.il<br>- cocacola.co.il<br>- xboxignite.co.il<br>- intel.co.il<br>- live.co.il<br>- msn.co.il<br>- skype.co.il<br>- cnn.co.il<br>- groupon.co.il |
| Nov 20 | Various Hackers | 🇮🇱 | The list of the websites defaced by variuous hackers under the umbrella of OpIsrael keeps on growing.[17] |
| Nov 20 | ANONYMOUS | 🇮🇱 | The Anonymous collective dumps personal information of 35,000 Israeli officials.[18] |
| Nov 21 | ZHC | | ZHC (zCompany Hacking Crew) hacks the Twitter and Facebook profiles belonging to Silvan Shalom, Israel Vice PM and "doxes" his personal data.[19] |
| Nov 21 | ANONYMOUS | 🇮🇱 | As part of OpIsrael, Anonymous Indonesia the Anonymous collective leaks more than 113,000 Israeli emails and passwords obtained by Anonymous Indonesia.[20] |
| Nov 21 | ANONYMOUS | | After the Gaza ceasefire, the Anonymous stand down immediately from all further cyber attacks upon the IDF or Israel and encourage all those cyber groups who joined them to also cease and desist from aggressive acts, "to give this cease-fire a chance".[21] |
| Nov 22 | Hannibal | | After the ceasefire there is a second example of an (alleged) cyber attack carried on by a Pro-Israeli hacker. Against OpIsrael. Hannibal, another contender of the Middle East Cyber War, releases what he claims to be a list of 1 million email accounts from American Citizens. The leak will be proven as false.[22] |

Hackmageddon.com