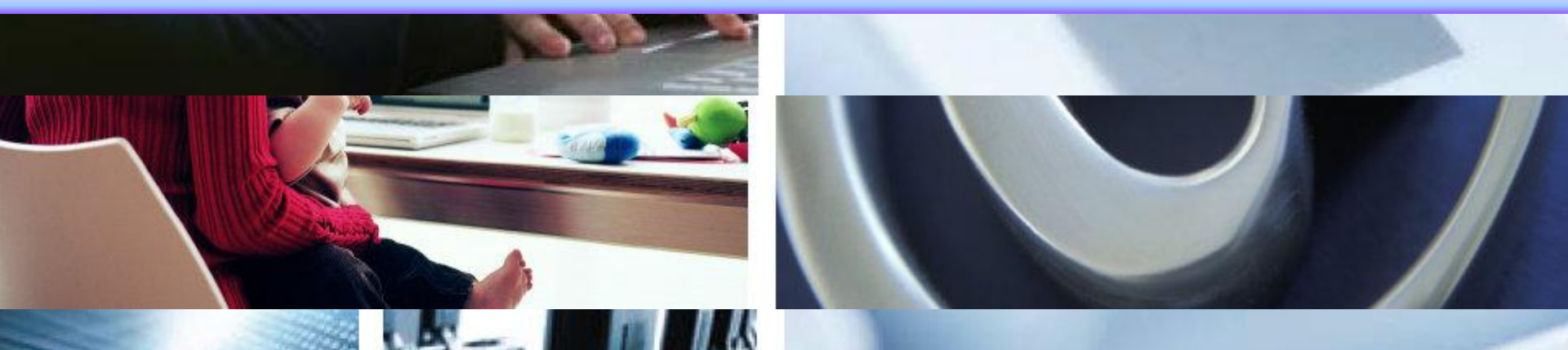
enisa
European Network and Information Security Agency

Getting the Cybersecurity Strategy Process Right

Dr. Frederick Wamala, CISSP®

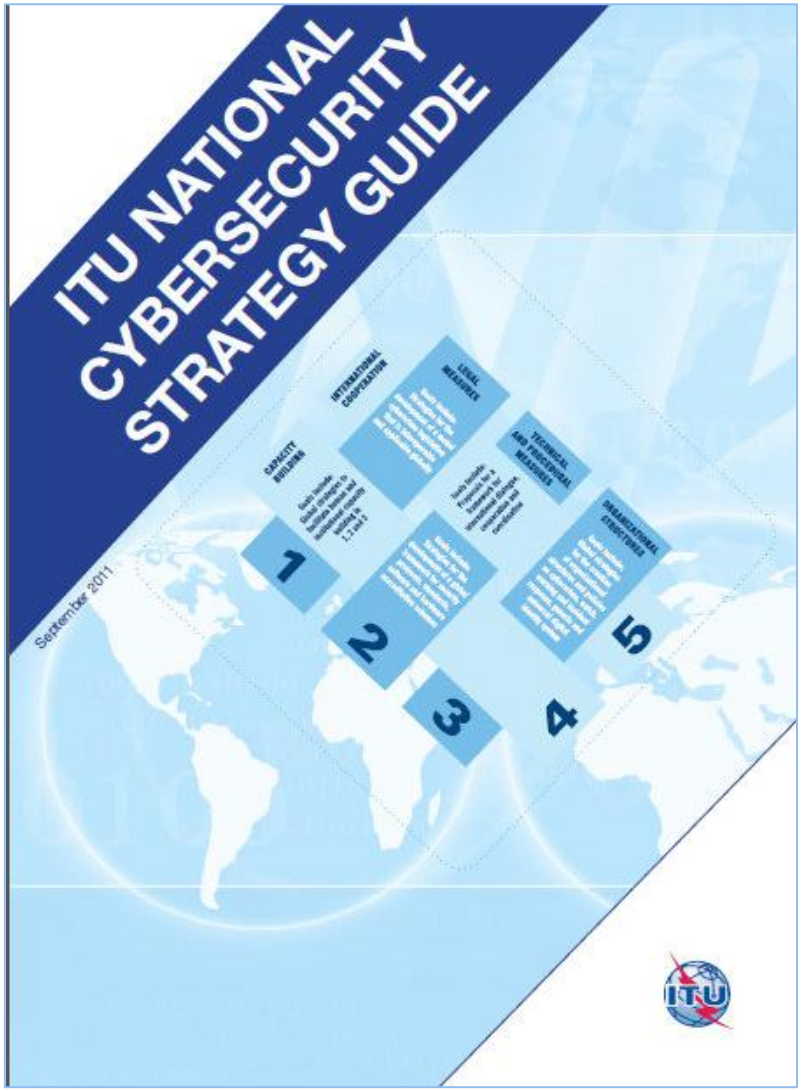
ENISA Cybersecurity Workshop, Brussels, 27 September 2012

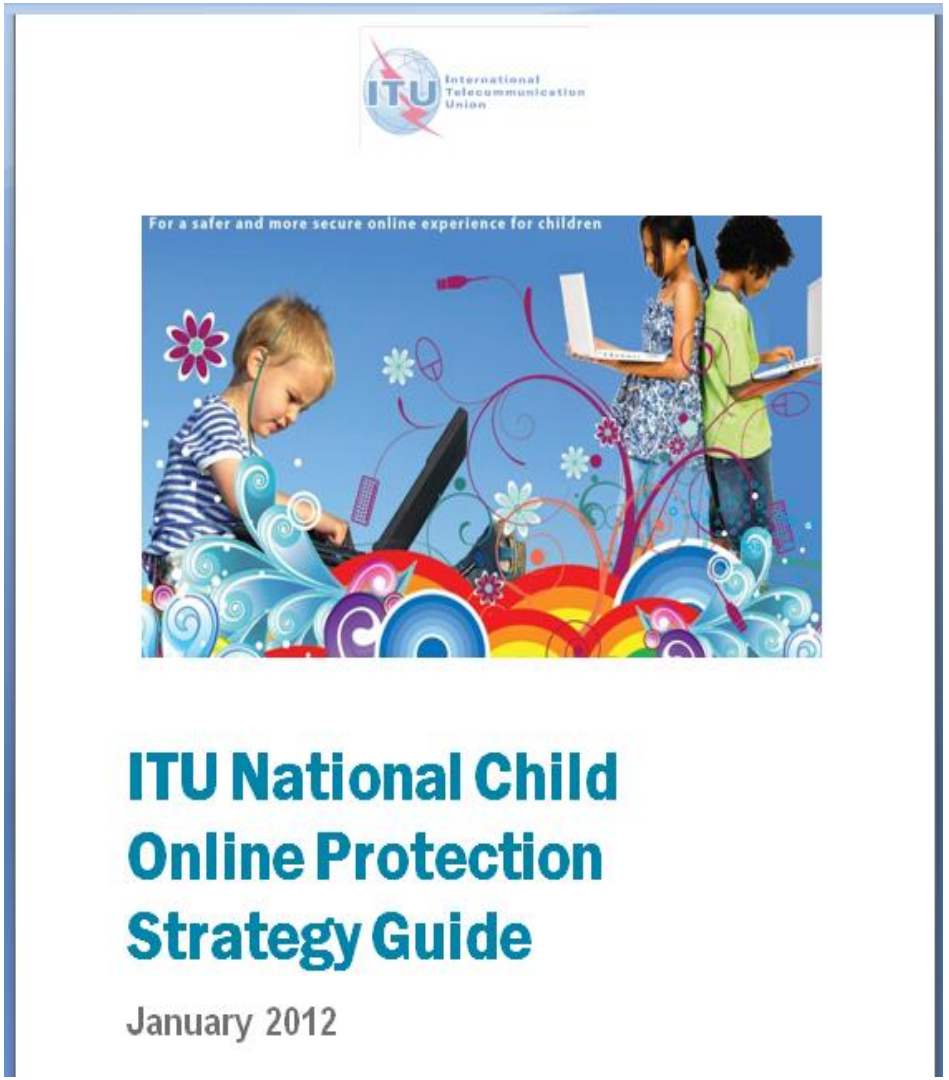


Disclaimer

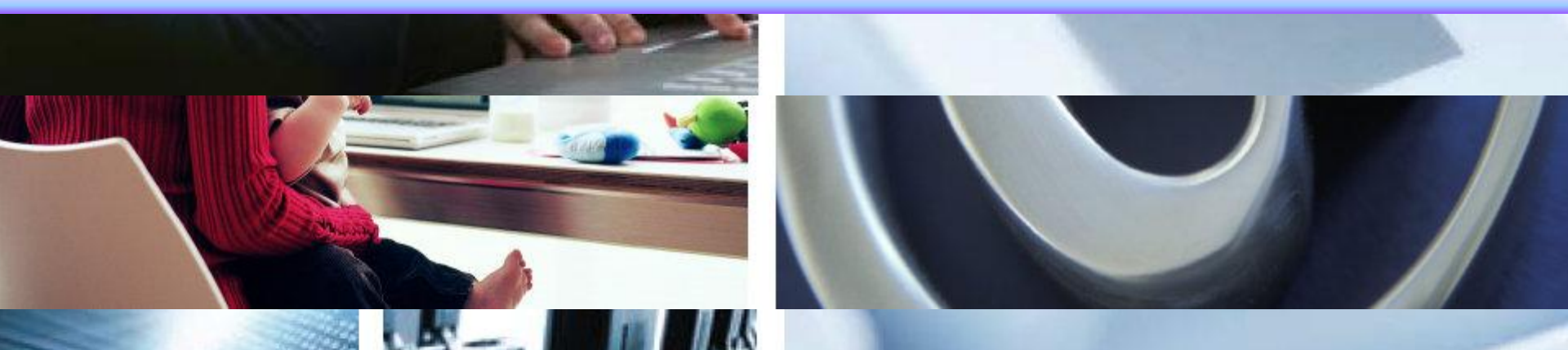
The views I express in this talk are mine and do not necessarily reflect the views of either past or present clients, employers and/or associates.

ITU Cybersecurity Strategy Guides





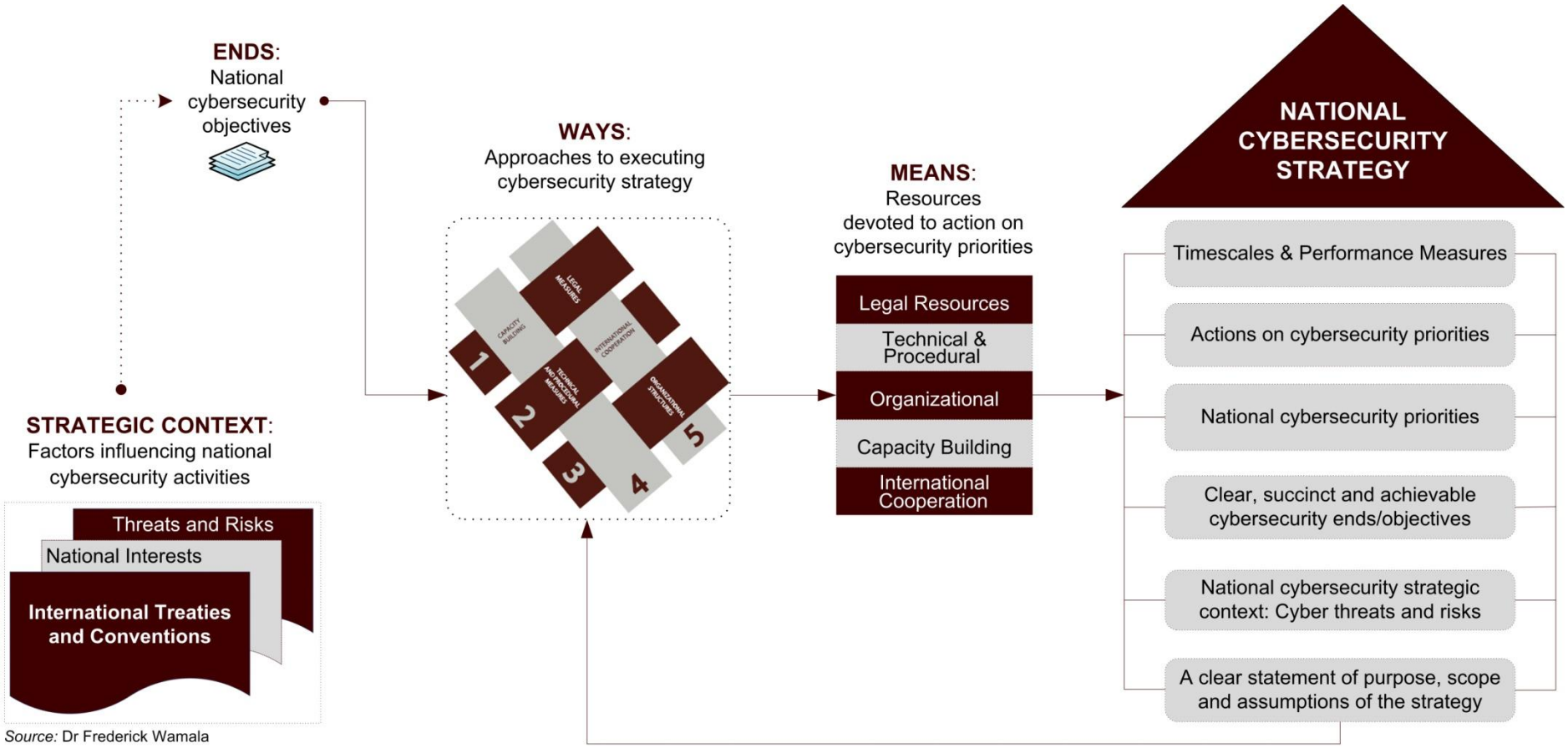
Strategy & Cybersecurity Strategy



Strategy

- **Strategy**
  - "Complex decision-making process that connects the **Ends** sought (objectives) with the **Ways** and the **Means** of achieving those ends," Drew and Snow (2006)
- **Cybersecurity Strategy**
  - "A **nationally-led** and **globally harmonised multi-stakeholder** effort to build human and institutional capacity to prevent, detect, react to and deter cyber threats and risks

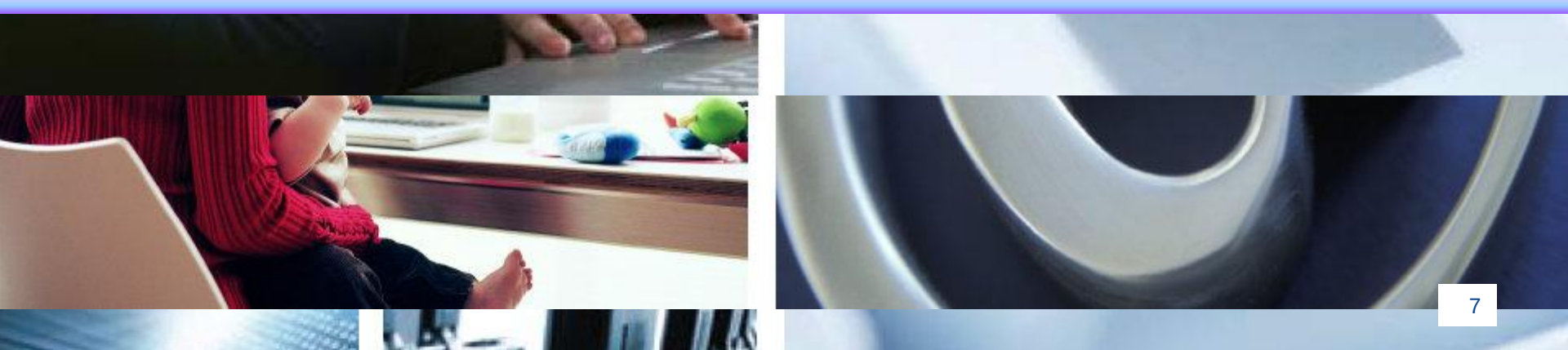
Cybersecurity Strategy Model



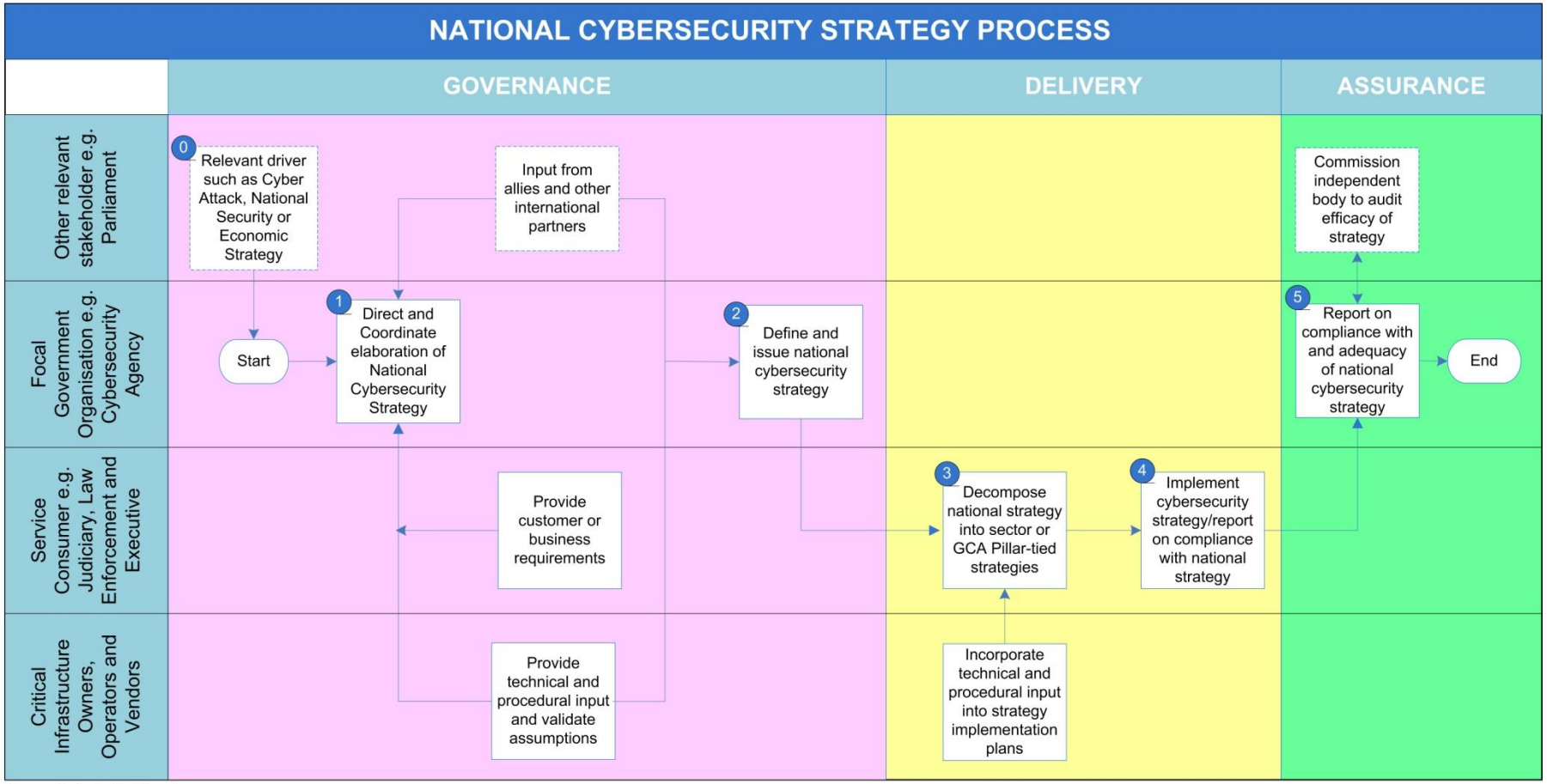
Source: Dr Frederick Wamala

URL: http://www.itu.int/ITU-D/cyb/cybersecurity/strategies.html

How to get started and how to define scope?



Strategy Development Process



Source: Dr Frederick Wamala

Source: Pages 31-33, **"ITU National Cybersecurity Strategy Guide"**

Ends – Goals Cybersecurity supports

Basic Interests at stake	Intensity of Interest: Survival	Vital	Major	Peripheral
Defense of Homeland				
Economic Well-being				
Favourable World Order				
Promotion of Values				

© Donald Neuchterlein

- Identify objectives **before** risk assessment
- Cyber attacks threaten ‘vital’ national interests

0 – Driver e.g. National Security

Technology Quarterly: Q4 2008

Cyberwarfare

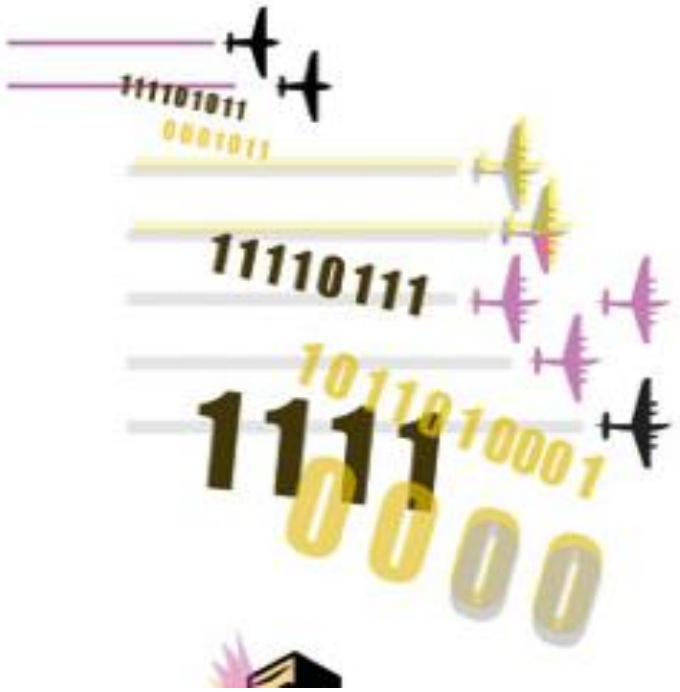
Marching off to cyberwar

The internet: Attacks launched over the internet on Estonia and Georgia highlight the difficulty of defining and dealing with "cyberwar"

Dec 4th 2008 | from the print edition

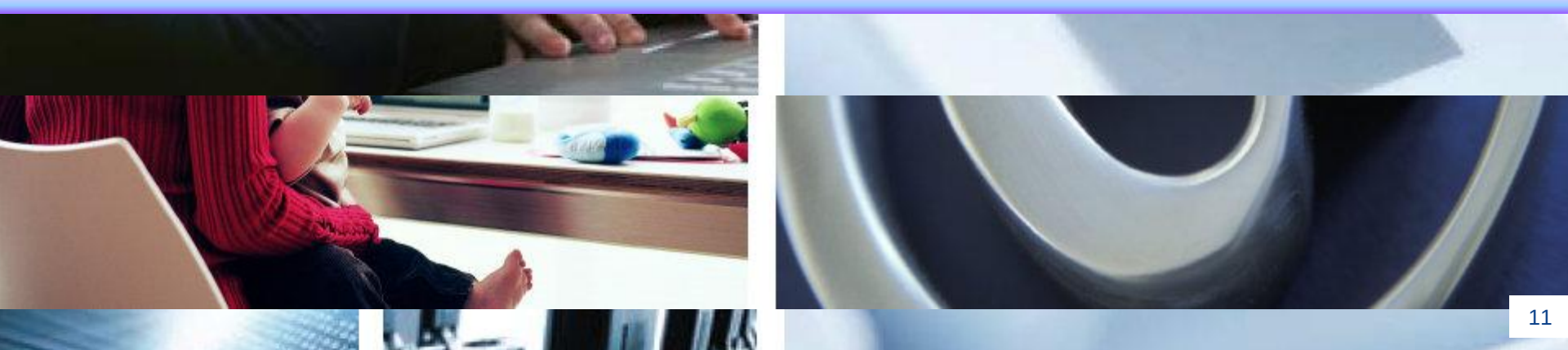
Like 3 Tweet 3

AS RUSSIAN tanks rolled into Georgia in August, another force was also mobilising—not in the physical world, but online. Russian nationalists (or indeed anyone else) who wished to take part in the attack on Georgia could do so from anywhere with an internet connection, simply by visiting one of several pro-Russia websites and downloading the software and instructions needed to perform a "distributed denial of service" (DDoS) attack. This involves sending a flood of bogus requests to an internet server, so that it is overwhelmed by the demand and becomes unusable.

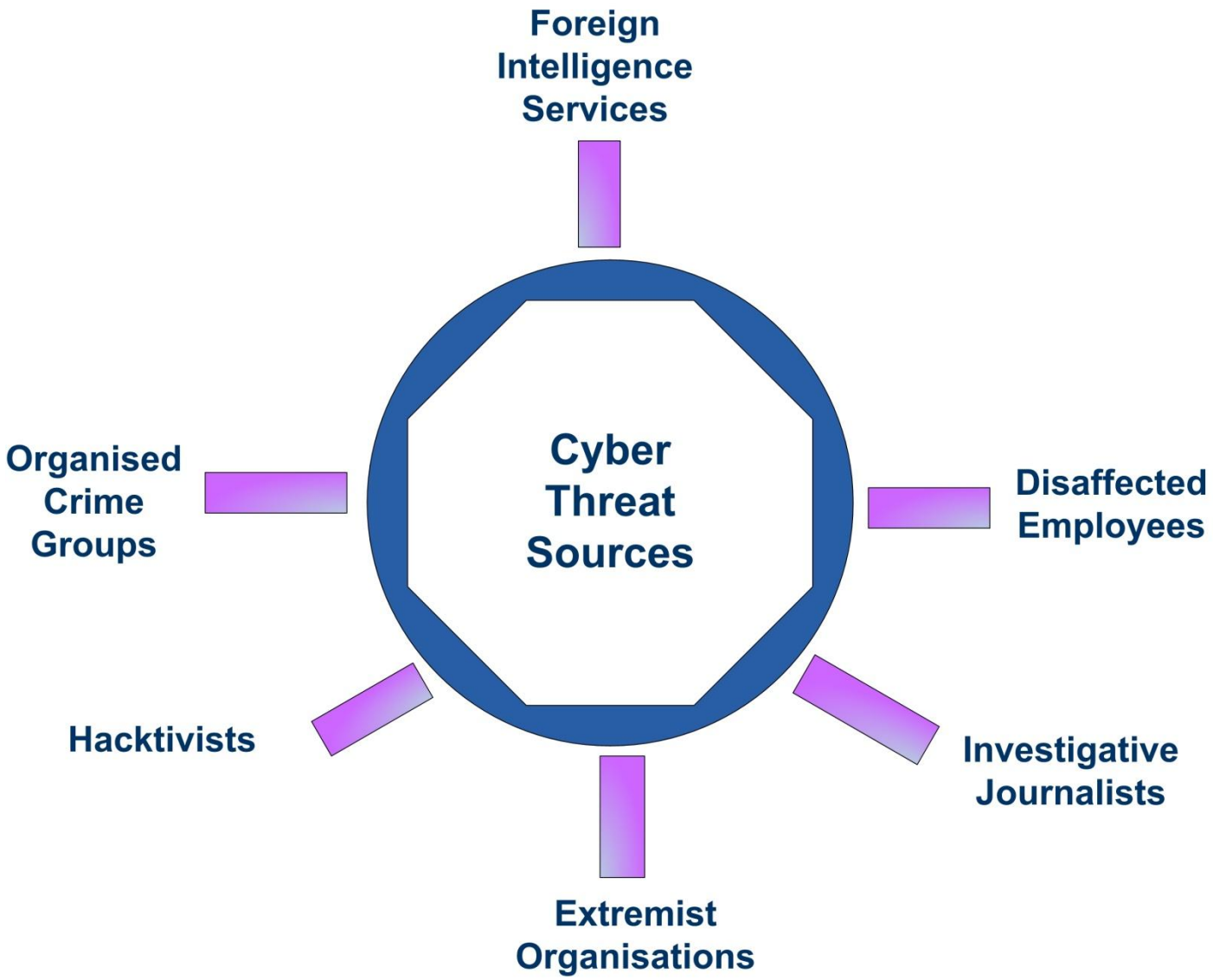


- **Source:** The Economist

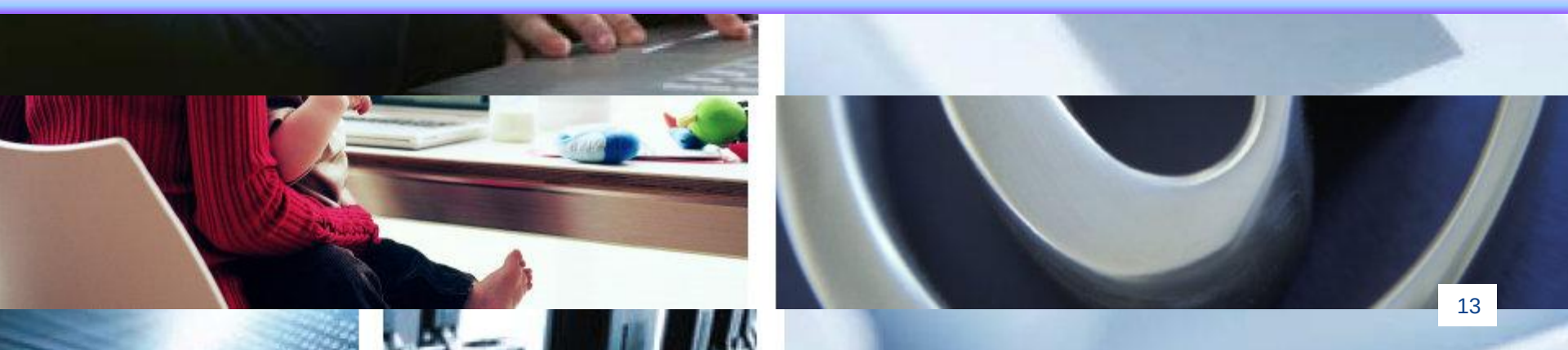
Threat Sources and Cyber Risks



Focus on threat sources NOT methods



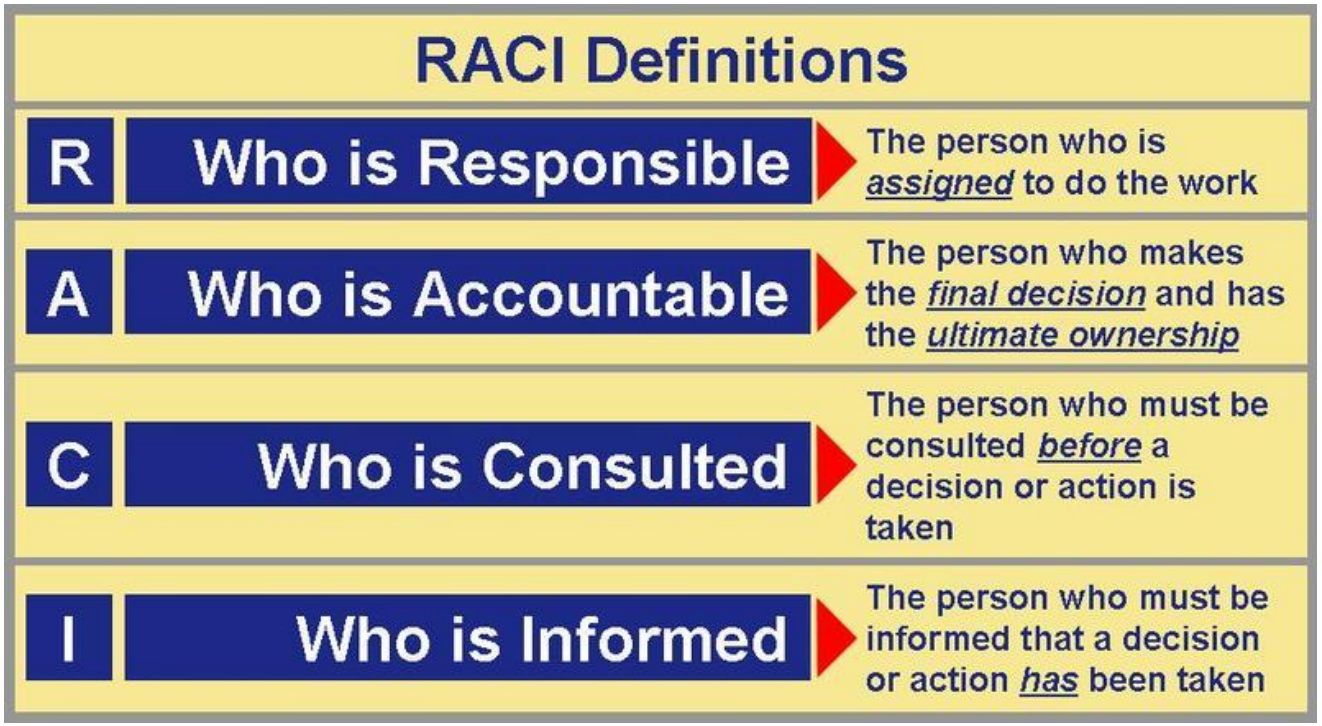
Who to involve and how?



Cybersecurity Stakeholders

- Executive Branch of Government
- Legislative Branch of Government
- Critical Infrastructure Owners and Operators
- The Judiciary
- Law Enforcement
- Intelligence Community
- Vendors
- Academia
- Citizens/civil society
- International partners

Governance Structures crucial



- Different cybersecurity objectives
- Government: **Accountable**
- Private sector: **Responsible** under the law

Governance – Government Leadership

- Set national cybersecurity agenda
- Sponsor national cybersecurity programme
- Maintain focus on cybersecurity priorities
- Cybercrime legislation
- Human and institutional capacity building
- Cybersecurity agreements and conventions
- International cooperation

US – Top Government Leadership

Napolitano: Executive order on cybersecurity is 'close to completion'

By Jennifer Martinez - 09/19/12 11:53 AM ET

COMMENT
EMAIL
PRINT
SHARE

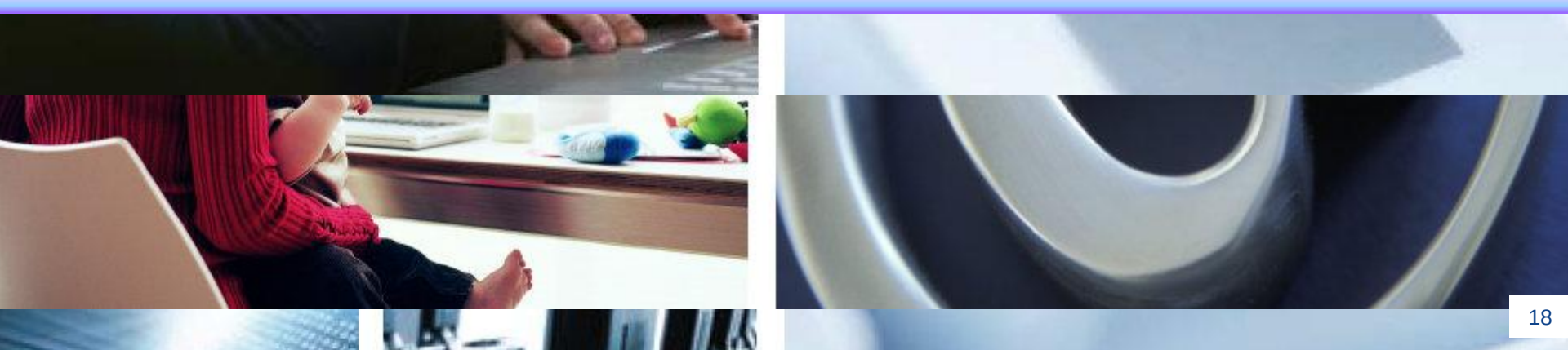
Tweet 336 Like 1.2k Send +1 18

Homeland Security Secretary Janet Napolitano on Wednesday said the cybersecurity executive order that the White House is drafting is "close to completion."

At a Senate Homeland Security and Governmental Affairs Committee hearing, Napolitano said the executive order is "still being drafted in the inter-agency process" and "is close to completion depending on a few issues that need to be resolved at the highest levels."

She said the draft order still needs to be reviewed by President Obama.

Create & Empower a National Focal Point



1 – "Coordinator" name NOT enough

Lawmakers question whether DHS cybersecurity role will be undercut by White House appointment

Department of Homeland Security nominee assures Senate hearing new role will not conflict

By Jaikumar Vijayan
June 4, 2009 05:44 PM ET

Add a comment + Briefcase

Computerworld - Just days after President Obama announced his plan to appoint a new White House cybersecurity coordinator, lawmakers are questioning the impact the move might have on the U.S. Department of Homeland Security's role in cybersecurity.

At a confirmation hearing on Wednesday for Rand Beers, the nominee for the undersecretary for the department's National Protection and Programs Directorate, members of the U.S. Senate Committee on Homeland Security and Governmental Affairs expressed hope the move wouldn't dilute DHS' cybersecurity mission.

Sen. Susan Collins (R-Maine), a ranking member of the Senate Committee, said she had a "lot of reservations about the establishment of a White House cybersecurity czar." Such an appointment would make it far more difficult for members of Congress to provide oversight because it would not be easy to get a presidential adviser to testify before the committee, she said.

JULY 30, 2012 | BY MARK M. JAYCOX AND LEE TIEN AND TREVOR TIMM

Why The NSA Can't Be Trusted to Run U.S. Cybersecurity Programs

This week, the Senate will be voting on a slew of amendments to the newest version of the Senate's cybersecurity bill. Senators John McCain and Kay Bailey Hutchison have proposed several amendments that would hand the reins of our nation's cybersecurity systems to the National Security Agency (NSA). All of the cybersecurity bills that have been proposed would provide avenues for companies to collect sensitive information on users and pass that data to the government. Trying to strike the balance between individual privacy and facilitating communication about threats is a challenge, but one thing is certain: the NSA has proven it can't be trusted with that responsibility. The NSA's dark history of repeated privacy violations, flouting of domestic law, and resistance to transparency makes it clear that the nation's cybersecurity should not be in its hands.

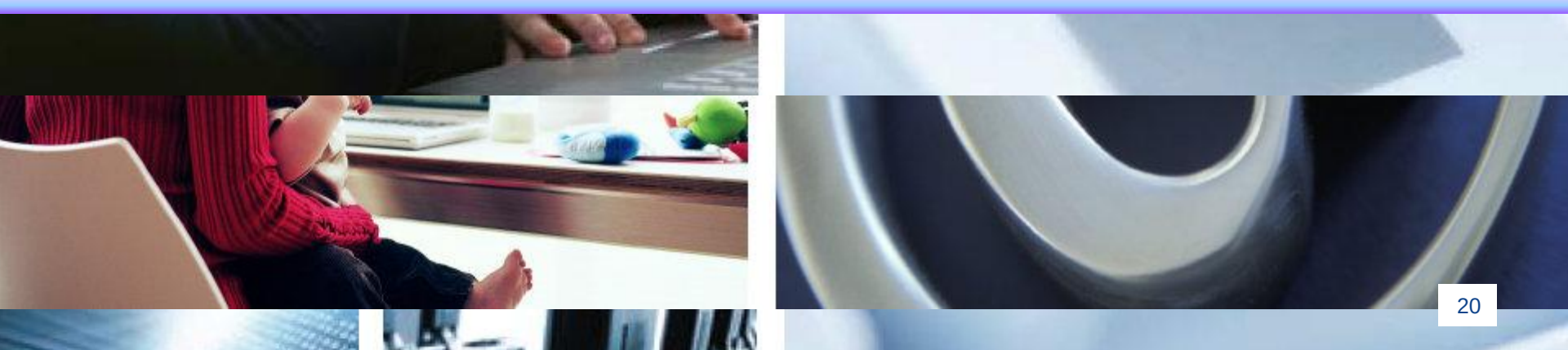
In case you need a refresher, here's an overview of why handing cybersecurity to the NSA would be a terrible idea:

1. **An executive order generally prohibits NSA from conducting intelligence on Americans' domestic activities**

   Executive Order 12333 signed by President Reagan in 1981 (and amended a few times since[1]), largely prohibits the NSA from spying on domestic activities:

   > no foreign intelligence collection by such elements [of the Intelligence Community] may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons.

Achieving commitment – Public-Private Partnership



Commitment – Value Proposition

- Private sector contribution (R, C and I)
  - Expert knowledge of cyber assets, networks etc
  - Incident response expertise
  - Innovate new secure systems and services
- Government contribution (Accountable)
  - Legal tools to boost collective security
  - Focus on issues of interest to the private sector
  - Cybersecurity research incentives
  - Information on critical infrastructure threats
  - Pre-requisite for doing business

Achieving Commitment – Build Trust

- Different agendas i.e. Profit, politics etc
- Parties must trust each other's motives
- Confidence in capacity to discharge duties
- Can private companies securely handle classified government data on cyber threats?
- Can the private sector trust government to protect commercially-sensitive data?
- Who is liable if collaboration breaches law?

UK – Public-Private Partnership

Defense Industrial Base Cyber-Pilot

U.S. DEPARTMENT OF DEFENSE

Search

HOME | TODAY IN DOD | ABOUT DOD | TOP ISSUES | NEWS | PHOTOS/VIDEOS | MILITARY/DOD WE

TOP LINKS

Subscribe
- Twitter
- AFPS Blogs
- Facebook
- Flickr
- RSS
- Podcasts
- Widgets
- E-Mail

Secretary of Defense
- Speeches
- Travels
- Messages
- Biography
- Other Top Leaders

Press
- Today in DoD
- News Releases
- Press Advisories
- Publications
- Transcripts

News

American Forces Press Service

SHARE

NEWS ARTICLE | E-MAIL A COPY | PRINTER FRIENDLY | LATEST NEWS

Lynn Outlines New Cybersecurity Effort

By John D. Banusiewicz
American Forces Press Service

PARIS, June 16, 2011 – Deputy Defense Secretary William J. Lynn III outlined a pilot program here today in which the government helps the defense industry in safeguarding the information their computer systems hold.

In a keynote address at the Center for Strategic Decision Research's 28th International Workshop on Global Security, Lynn described Defense Industrial Base Cyber Pilot -- called "DIB Cyber Pilot" for short -- in which the Defense Department, in partnership with the Department of Homeland Security, shares classified threat information and the know-how to employ it with participating defense companies or their Internet service providers to help them in defending their computer networks from attack or exploitation.

"Our defense industrial base is critical to our military effectiveness. Their networks hold valuable information about our weapons systems and their capabilities," Lynn said. "The theft of design data and engineering information from within these networks greatly undermines the technological edge we hold over potential adversaries."

Current countermeasures have slowed exploitation of U.S. defense industry networks, but haven't stopped it, the deputy secretary told the audience, leading to DIB Cyber Pilot's establishment last month with a handful of defense-industry companies, all of which volunteered for the program.

Dr. Frederick Wamala, CISSP®
Cybersecurity Adviser
– Strategic and Technical

E-mail: f.wamala@efrivo.com
Twitter: @DrWamala