SYNAPTIC LABORATORIES LTD.

Synaptic Laboratories Ltd's Annual Report on the Global Cyber Security Status

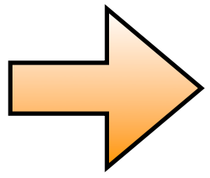
6 February 2012

The Current International Cyber Context We Work In

Escalating Regional National and Commercial Risks

Watch this presentation as a streaming video online:
http://www.synaptic-labs.com/resources/streaming-videos/synaptic-labs-2012-annual-reports-video-series.html

Synaptic Labs' Annual Report on the Global Cyber Security Status 2012

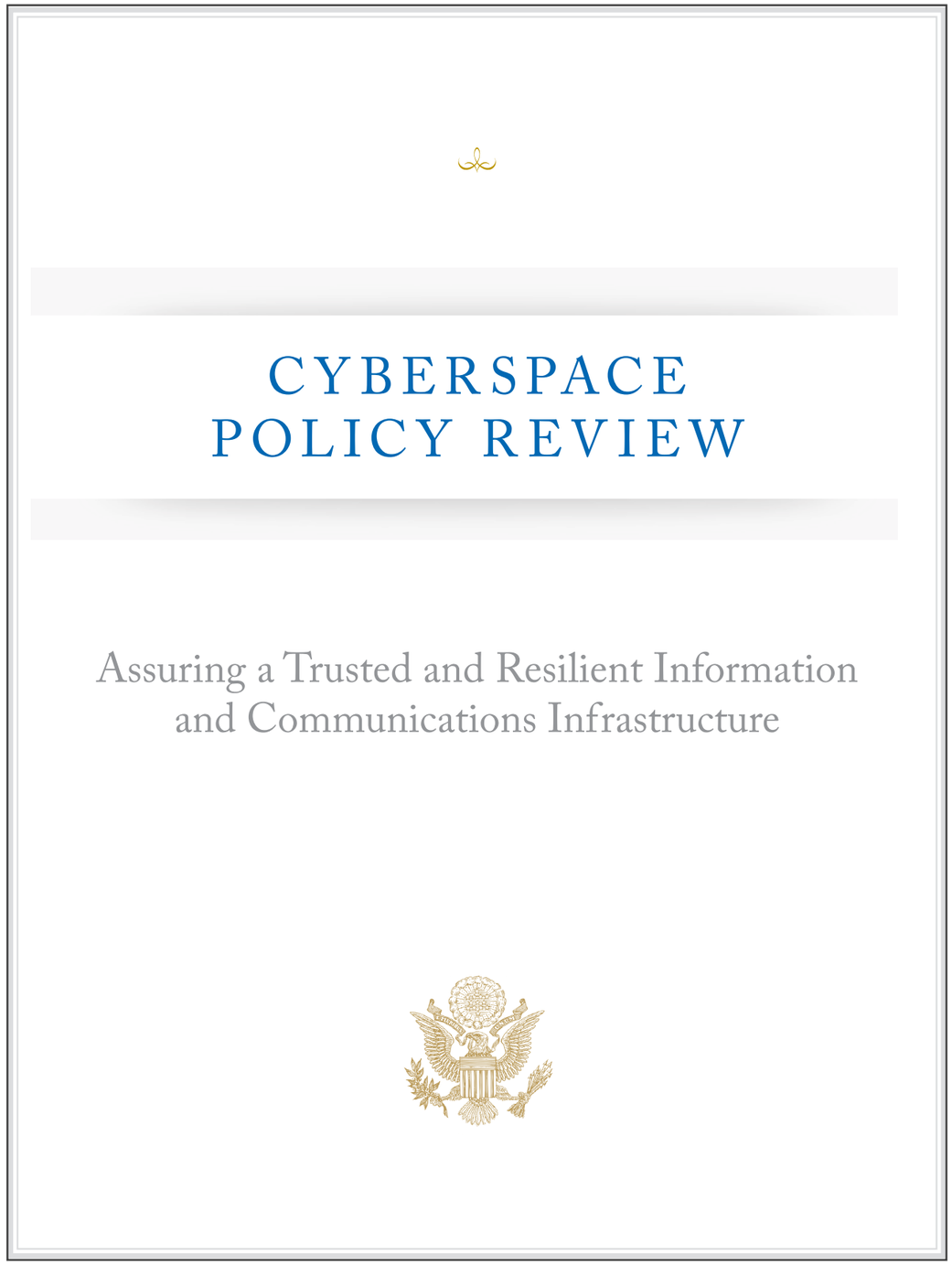


1. **High level overview**
2. Global assessments and global responses
3. The stability of Nations is at risk
4. Our cyber defences are very low
5. Experts: The cyber risk is not overstated
6. Closing statement
7. Related videos

What is cyberspace and why is it so important?

US Government
Cyberspace Policy Review

"The globally-interconnected **digital information and communications infrastructure** known as **"cyberspace" underpins almost every facet of modern society** and provides **critical** support for the U.S. economy, civil infrastructure, public safety and national security."



Internet and ICT delivers prosperity at the cost of dependency

- **Transforming the world very quickly**
- **Enabling the global village**
  - **inter**-connected
  - **inter**-dependent
- **Strengthening open societies**
- **"Playing a vital role in driving prosperity ...**
  21% of GDP growth in the last five years in 'mature' countries."
  - McKinsey Global Institute, Internet Matters, **2011**
- **PROBLEM: Cyber DEPENDENCY had no prior risk management**

We have to correct our mistakes

- Generally speaking, the Internet and ICT have been deployed without adequate dependency risk assessment
- Products rushed to market for higher performance and lower cost
  - Sacrificing quality, reliability, safety and security
  - Products engineered using the wrong or inadequate security practices
  - Little concern for “roll-on” costs to stakeholders as a result of failures

We have to correct our mistakes

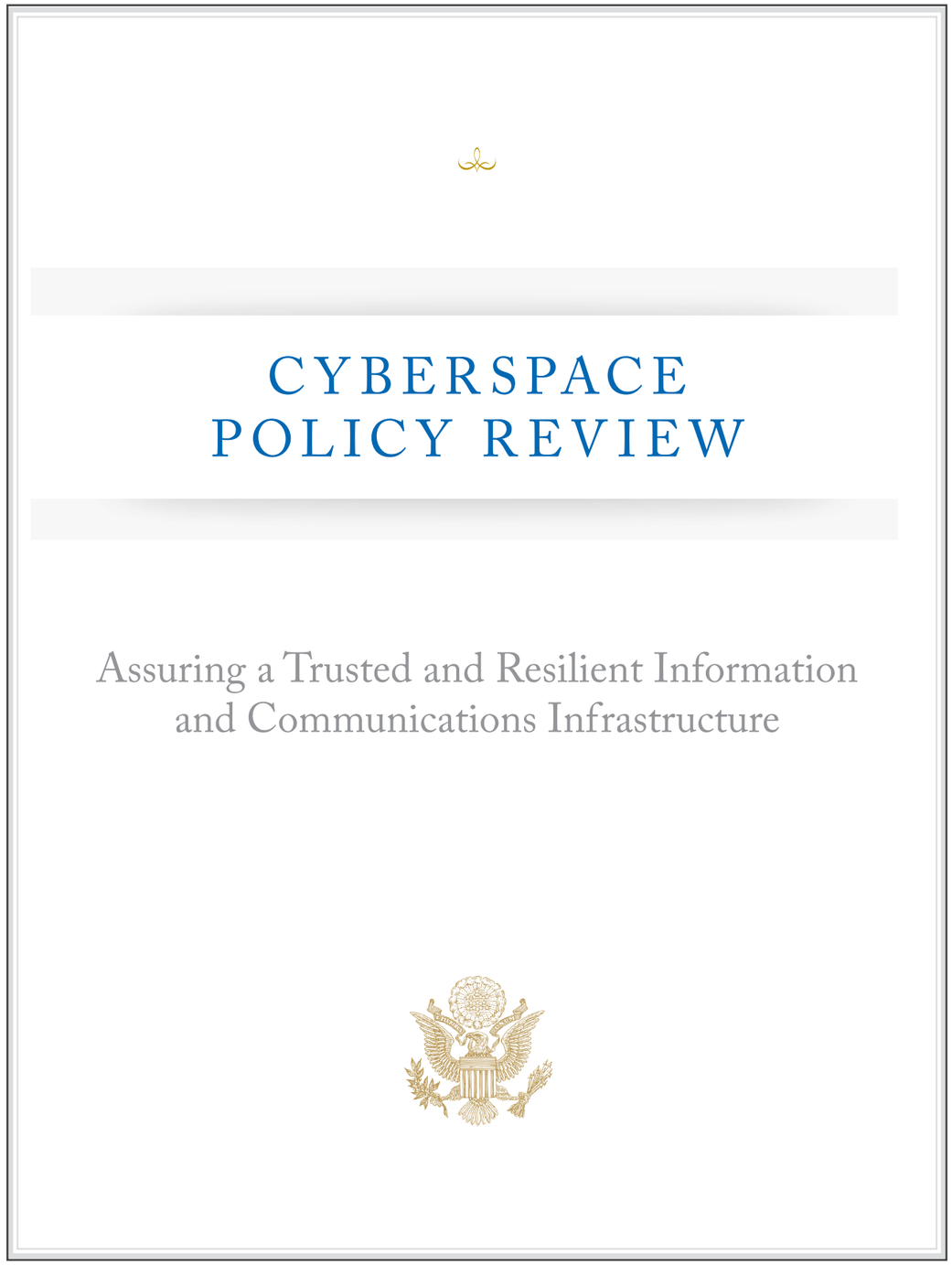
- This lack of assurance is now the focus of global attention as the escalating risks become apparent and begin to bite
- International inter-connectivity and inter-dependence demands uniform end-to-end security for all stakeholders
- **URGENT NEED** to converge and deliver ‘safety’ and ‘security’ in ICT

SERIOUS cyber dependency problems

US Government Position
Cyberspace Policy Review

"**Great risks** threaten nations, private enterprises, and individual rights ...

The architecture of the Nation's digital infrastructure, based largely upon the Internet, **is not secure or resilient.**"


CYBERSPACE
POLICY REVIEW

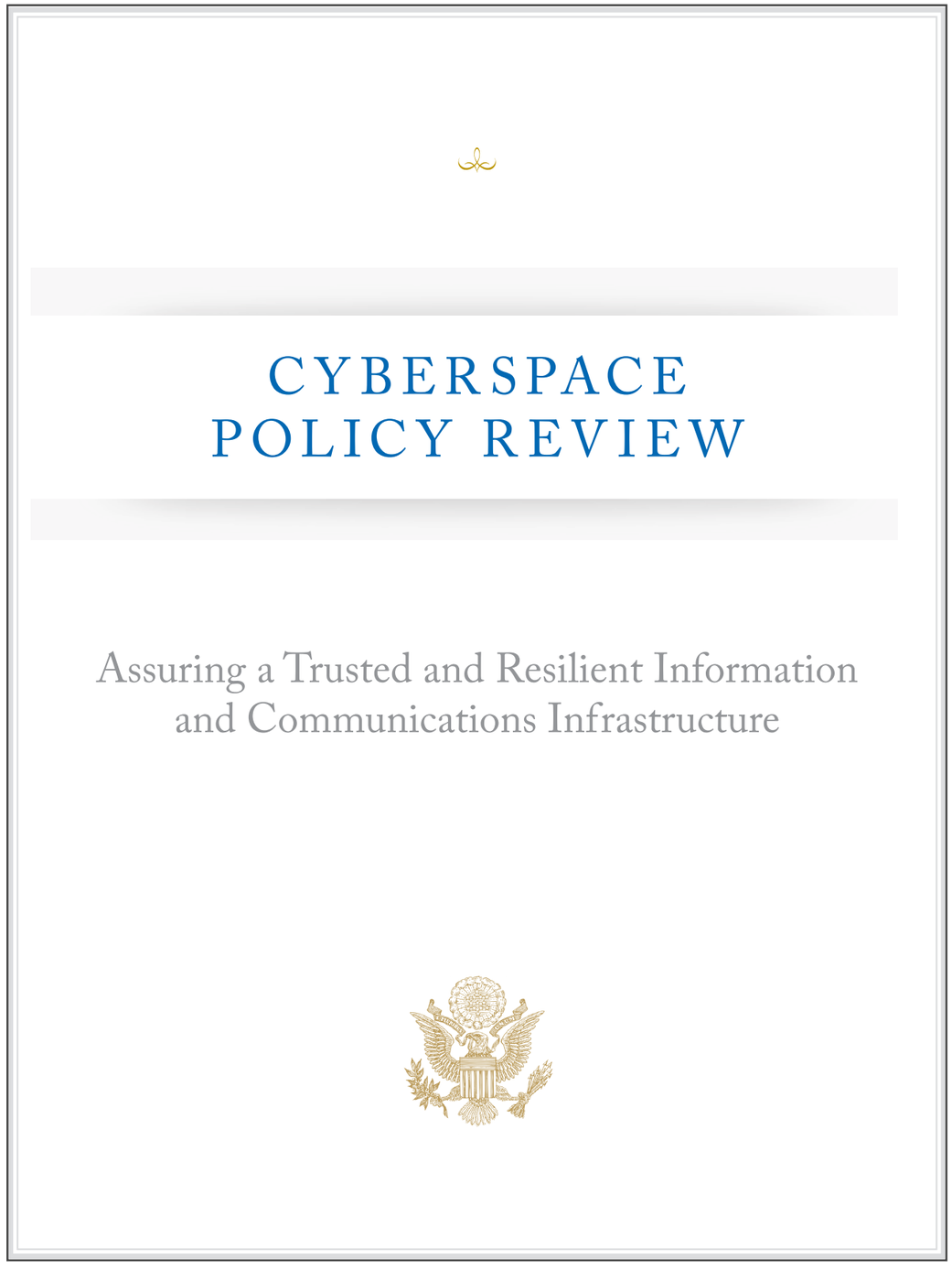
Assuring a Trusted and Resilient Information and Communications Infrastructure

SERIOUS cyber dependency problems

US Government Position
Cyberspace Policy Review

"The .. dialogue on cybersecurity must begin today."

"People cannot value security without first understanding how much is at risk."

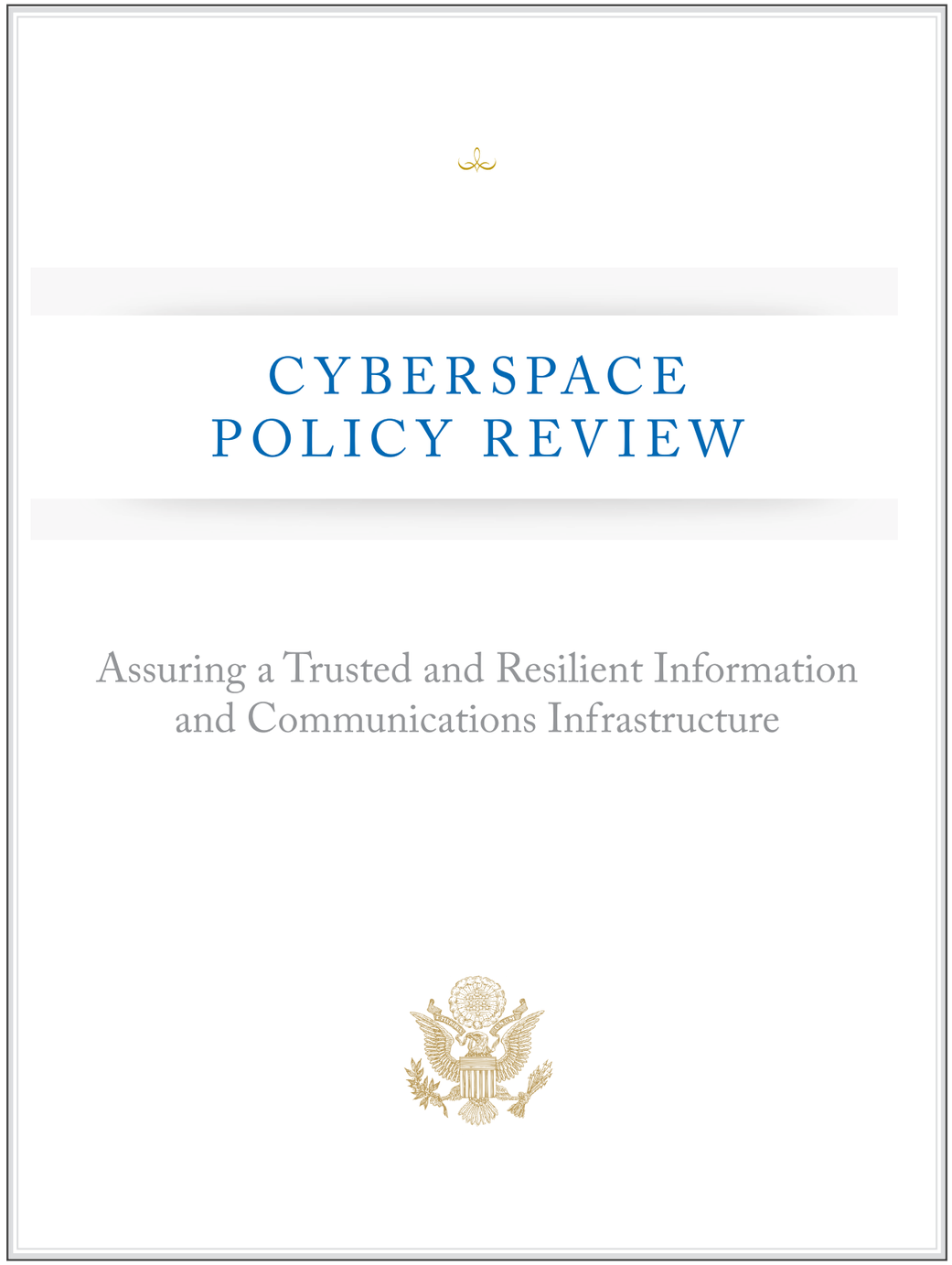


SERIOUS cyber dependency problems

US Government Position
Cyberspace Policy Review

"It's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation.

It's also clear that we're not as prepared as we should be, as a government or as a country."


CYBERSPACE
POLICY REVIEW

Assuring a Trusted and Resilient Information and Communications Infrastructure

Introduction to Brian Snow

35 years in the USA NSA

- **20 years doing and directing research** and development of cryptographic components and secure systems
- **12 years as Technical Director**
  - Research Directorate (1994-1995)
  - Information Assurance Directorate (1996-2002)
  - Directorate for Education and Training NSA's Corporate University (2003-2006)
- **Many cryptographic systems** serving the U.S. government and military **deploy his algorithms**; they ... span a range from nuclear command and control to tactical radios for the battlefield

Poor Cyber Security Practice

"There are problems today in Cyber Security practice that **impact the community as a whole,** and we need to solve those problems soon.

They are pervasive, ongoing, and getting worse, not better."

"Right now, the community at large is applying the **wrong or inadequate engineering practices**, and taking a lot of short cuts.

This adds greatly to our collective security risks."

Brian Snow
Our Security Status is Grim
Former US NSA, 35 years incl.
Technical Director (R&D, IAD, ADET)

SERIOUS cyber dependency problems

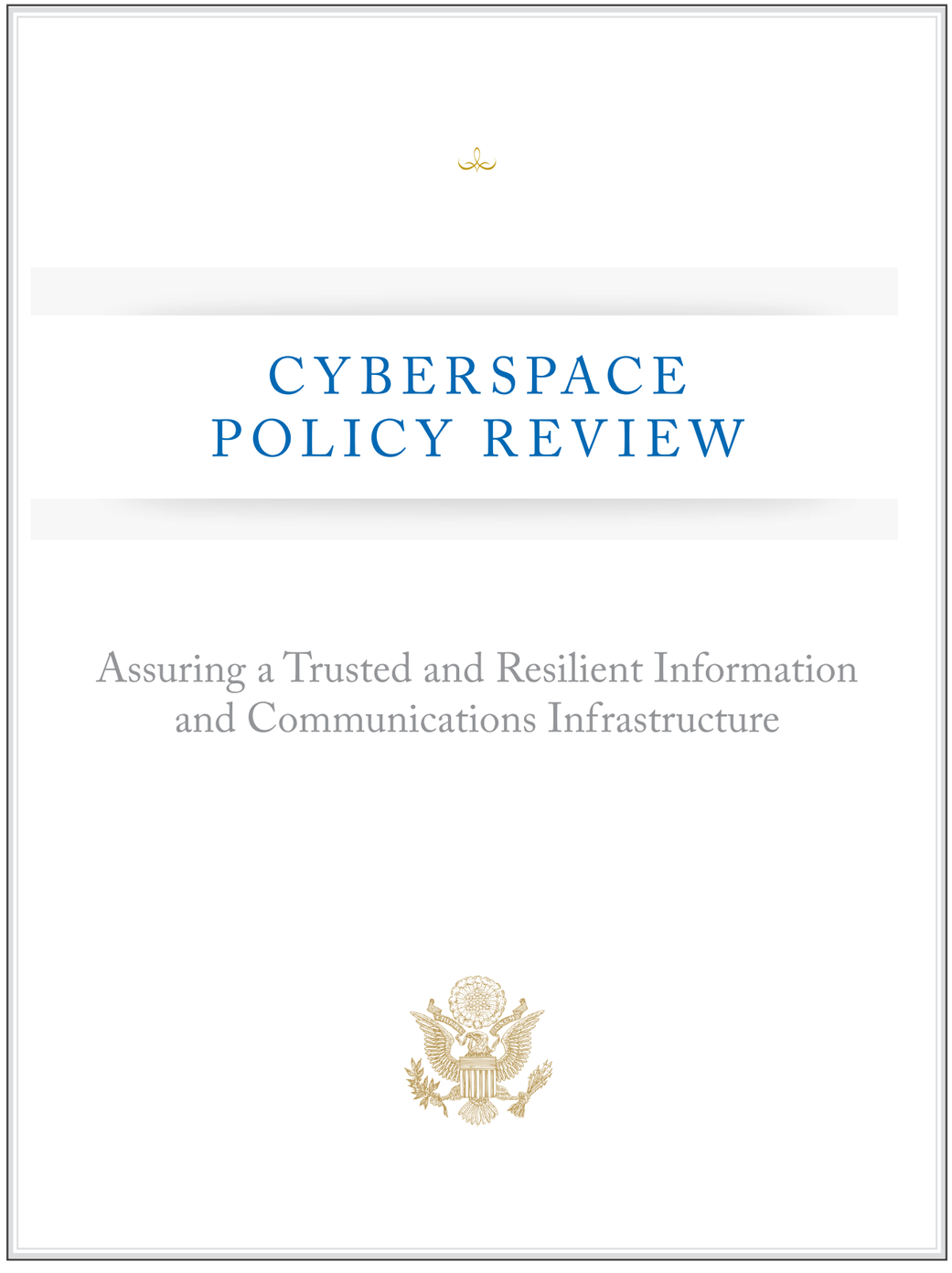
US Government Position
Cyberspace Policy Review

“This status quo is no longer acceptable -- not when there's so much at stake.

We can and we must do better.

Given the **enormous damage** that can be caused by even **a single cyber attack**, ad hoc responses will not do.

[It is not] sufficient to simply strengthen our defences after incidents or attacks occur.”


CYBERSPACE
POLICY REVIEW

Assuring a Trusted and Resilient Information and Communications Infrastructure

SERIOUS cyber dependency problems

UK Government Position
Cyber Security Strategy 2011

"Cyberspace has now grown to become a domain where strategic advantage – **industrial** or military – can be won or lost.

It **underpins** the complex systems used by **commerce** (e.g. **banking,** the delivery of **food** and the **provision of utilities such as power and water**) and the military.

The growing use of cyberspace means that its disruption can affect nations' ability to function effectively in a crisis."

SERIOUS cyber dependency problems

UK Government Position
Cyber Security Strategy 2011

"The covert nature of the threat means that the public and businesses can underestimate the risks."

➠ **"Companies are carrying far too much risk!"**

– **Robert Quick**
CEO BlueLight Global Solutions
former Assistant Commissioner (Specialist Operations) of London's Metropolitan Police Service responsible for counter terrorism within the UK

There is international consensus

- MANY comprehensive cyber security reports **published by Governments, large cyber security organizations and industry experts** are readily available to the public

  - US Govt. Cyberspace Policy Review, 2009
  - US Govt. International Strategy for Cyberspace, 2011
  - US Gov. Accountability Office, “United States Faces Challenges in Addressing Global Cybersecurity and Governance”, 2010
  - UK Govt. Cyber Security Strategy, 2009, 2011
  - EU Commission funded FP7 RISEPTIS and ThinkTrust reports
  - O. Sami Saydjari, 2007 Testimony to Congress
  - Cisco Annual Security Reports 2010, 2011
  - McAfee annual critical infrastructure protection reports 2010, 2011
  - CNAS, “America’s Cyber Future”, 2011
  - and more

The international consensus is:

Collaborative corrective action must be taken NOW by all sectors to:

1. Maintain **public confidence** in existing ICT enabled systems
2. **Support the uptake of future ICT enabled advances such as cloud computing that promise massive societal benefits**

"The trustworthiness of our increasingly digitised world is at stake."

EU Commission funded FP7 RISEPTIS Report 2011

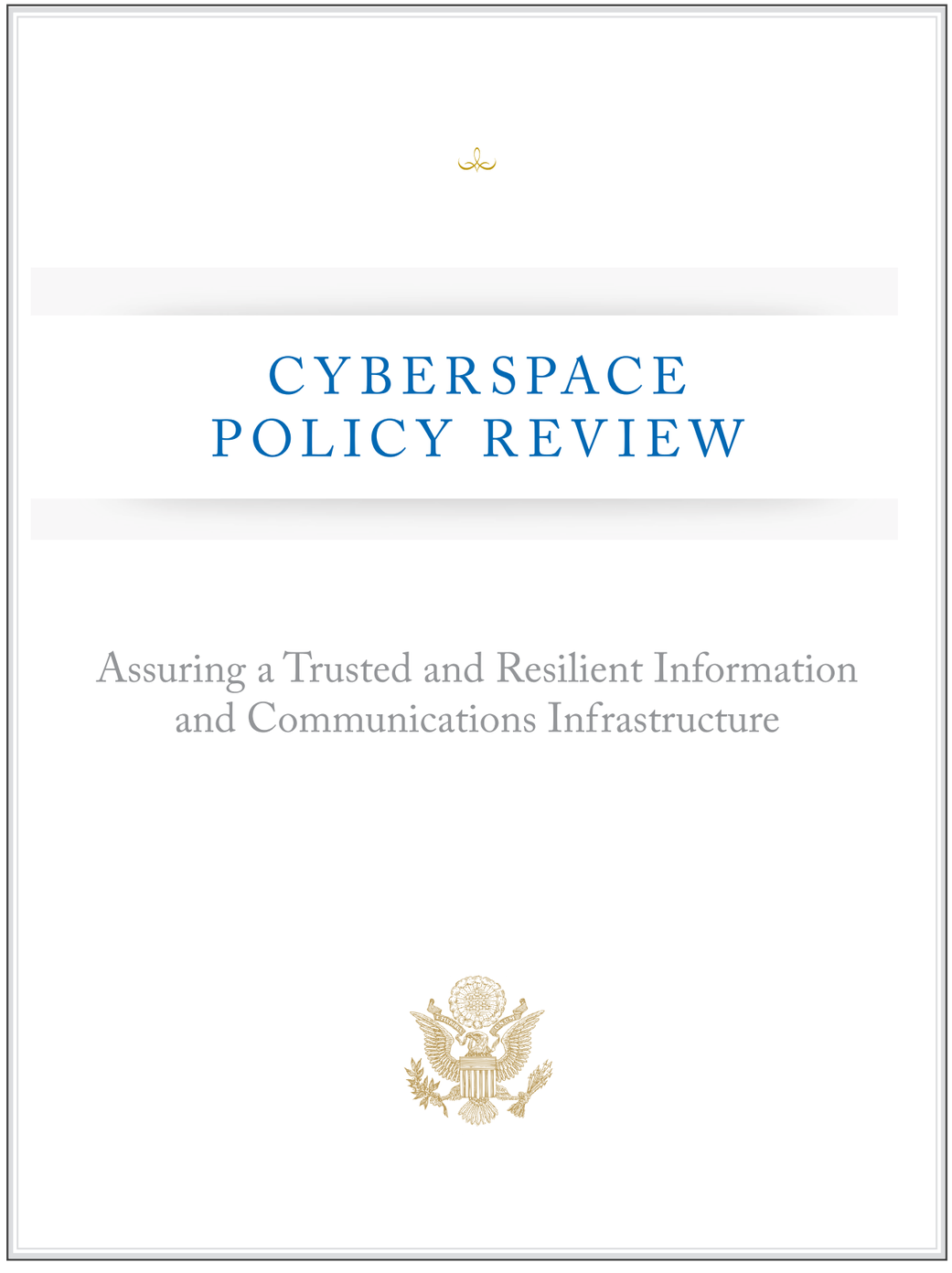
Public confidence must be maintained

US Government Position
Cyberspace Policy Review

"Information technology has transformed the global economy and connected people and markets in ways never imagined.

To realize the full benefits of the digital revolution, users must have confidence that sensitive information is secure, commerce is not compromised, and the infrastructure is not infiltrated.

Nation-states also need confidence that the networks that support their national security and economic prosperity are safe and resilient."



UK Government now pushing insurance drivers

UK Government Position
Cyber Security Strategy 2011

Action item 1.14:

> **"Work with business services providers (including insurers, lawyers and auditors) to discuss how they can develop the services they offer to businesses to help them manage and reduce the risks."**

EU increases focus on data protection

- **Major review of EU data protection**
  - 2009 ➔ ongoing
  - Modernise the EU legal system for the protection of personal data
  - http://ec.europa.eu/justice/policies/privacy/review/index_en.htm
- President of the EU hosts international data protection conference in 2011 as **sweeping changes are considered**
  - www.eu2011.hu/event/annual-meeting-agents-court-justice-eu

Governments propose heavy fines for security failures

- **26 January 2012:**
  EU Data Protection Law proposed amendment published

  Companies found to have mishandled any personal data they hold – be it of their customers, suppliers or their own employees – will face **"penalties of up to €1 million or up to 2% of the global annual turnover of a company"**

  http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

The risk can be turned to advantage

Incentives for strong commercial cyber security go far beyond risk management

Economic opportunities in strong cyber defence

- Cyber security is now seen as a huge growth market
- Driven by massive Government spending
- Driven by increasing demands and mandates for improved cyber security

- US President Barack Obama:

“Economic prosperity in the 21st century will depend on cyber security”

Economic opportunities in strong cyber defence

UK Government Position
Cyber Security Strategy - **December 2011**

"NATO Lisbon Summit highlighted the cyber domain as an area of significant new risk and opportunity for the Alliance."

"We will turn the threat into opportunity and make strong cyber security a positive for all UK businesses and part of the UK's competitive advantage."

The UK Cyber Security Strategy
Protecting and promoting the UK in a digital world

NATO OTAN

LISBONNE
SUMMIT 19-20 XI 2010 SOMMET

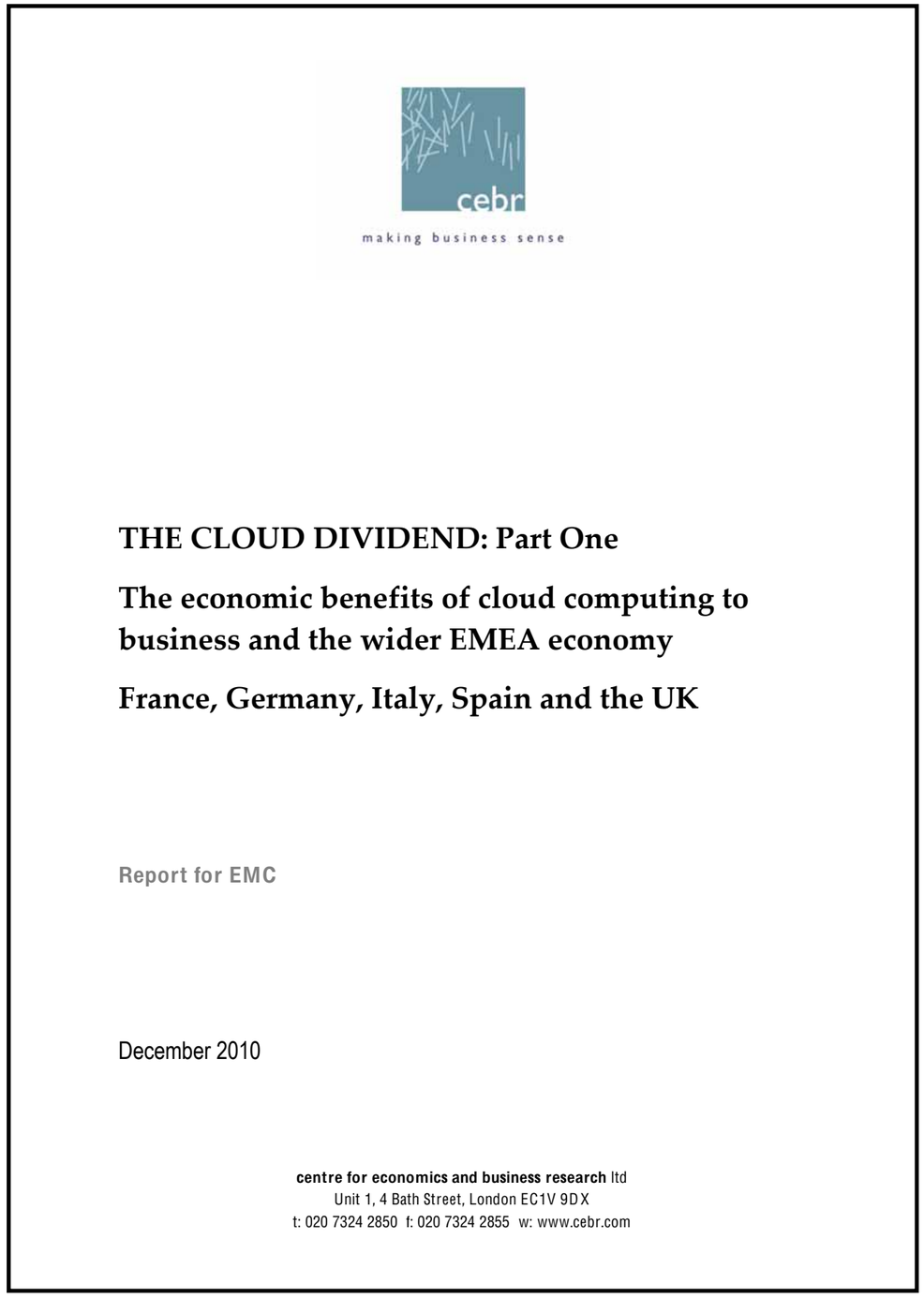
Unlock new markets with next gen. cyber security

- **Today's public clouds are not trustworthy or dependable enough**

- Centre for Economic and Business Research Report commissioned by EMC:

"Widespread **adoption of cloud computing** [across France, Germany, Italy, Spain and the UK], has the **potential to generate over €763 billion of cumulative economic benefits and hundreds of thousands of new jobs**"

"**53% of organisations that have NOT adopted the cloud cited confidentiality and security related issues as their primary concern.**"



cebr
making business sense

THE CLOUD DIVIDEND: Part One

The economic benefits of cloud computing to business and the wider EMEA economy

France, Germany, Italy, Spain and the UK

Report for EMC

December 2010

centre for economics and business research ltd
Unit 1, 4 Bath Street, London EC1V 9DX
t: 020 7324 2850 f: 020 7324 2855 w: www.cebr.com

Economic opportunities in strong cyber defence

UK Government Position
Cyber Security Strategy - **December 2011**

"Our vision is for the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace."

"In order to secure the vast economic and social benefits that cyberspace will offer the UK **we will transform our approach to cyber security**."

"The private sector has a crucial role to play in the UK's cyber security."

Can you size the market?

The Atlantic and Government Executive's Cybersecurity Forum, Dec 2010

“Size.. Probably the easier way to think about it is the information technology market. ... its measured in the trillions.

What ever happens to IT, I would assert the same thing is going to happen to cyber security.

I think of cyber security as the enabler to allow us to continue to enjoy this IT revolution.”

(video footage used with permission)

Vice Admiral J. Mike McConnell (USN Ret)
Intelligence Adviser to President Obama 2009

Can you size the market?

“If I look at it in Government terms, and just add up the numbers, it is probably on the order of 10-15 billion per year.

But if you look at it broadly across the commercial space I would say ... ~150 billion, and whatever happens with IT, cyber security will be pulled right there, because again it becomes the enabler.

So this is big business, and we are just now recognising it to the point where we are putting major resources against it.”

Vice Admiral J. Mike McConnell (USN Ret)
Intelligence Adviser to President Obama 2009

Synaptic Labs' Annual Report on the Global Cyber Security Status 2012

1. High level overview
2. **Global assessments and global responses**
3. The stability of Nations is at risk
4. Our cyber defences are very low
5. Experts: The cyber risk is not overstated
6. Closing statement
7. Related videos

Global risk, global responsibility, united in action

- Being interconnected and interdependent means that **cyber security is a shared responsibility** at home and in the global village
- Most nations have joined international cyber security efforts
- Many have launched national cyber awareness campaigns to engage the public

IMPACT
INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

COMNET
Foundation for ICT Development

United Nation's perspective

- The Secretary-General of the International Telecommunication Union (ITU) called for global cooperation to ensure security in cyberspace:

  "**The next world war could take place in cyberspace**"

- Traditional diplomacy between nation states may not be able to prevent cyberwar:

  "There is no such thing as a superpower in cyberspace because every individual is a superpower.

  It's the human brain that makes a difference in this field.

  Intelligence is a natural resource that is equally distributed everywhere in the globe."

  – Dr. Hamadoun Touré Secretary General of the ITU

UK Government: Cyber attack attribution problem

- You cannot *physically threaten* or *retaliate* against a person or state you cannot identify or hold liable!

"**All these different groups – criminals, terrorists, foreign intelligence services and militaries – are active today against the UK's interests in cyberspace.**"

The UK Cyber Security Strategy
Protecting and promoting the UK in a digital world

November 2011

UK Government: Cyber attack attribution problem

- You cannot *physically threaten* or *retaliate* against a person or state you cannot identify or hold liable!

"with the borderless and anonymous nature of the internet, precise attribution is often difficult and the distinction between adversaries is increasingly blurred."

"Some states regard cyberspace as providing a way to commit hostile acts 'deniably'."

The UK Cyber Security Strategy
Protecting and promoting the UK in a digital world

November 2011

International co-operation in cyberspace: United Nations

- **International Multilateral Partnership Against Cyber Threats (ITU - IMPACT)**
  - The cyber security executing body for the United Nations' International Telecommunication Union (ITU)
  - Headquarters - Malaysia
  - **The largest global cyber security alliance - 137 member nations**
  - www.impact-alliance.org

IMPACT
INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

International co-operation in cyberspace: North Atlantic Treaty Organization (NATO)

- **New NATO Strategic Concept** 2011
  - **"Develop further our ability to prevent, detect, defend against and recover from cyber-attacks**, including by using the NATO planning process to enhance and coordinate national cyberdefence capabilities, **bringing all NATO bodies under centralized cyber protection**, and better integrating NATO cyber awareness, warning and response with member nations".

- **NATO Heads of State and Government committed to an ambitious work plan to bolster NATO's cyber capabilities**

"There simply can be no true security without cyber security."

– Anders Fogh Rasmussen
NATO Secretary General
2011

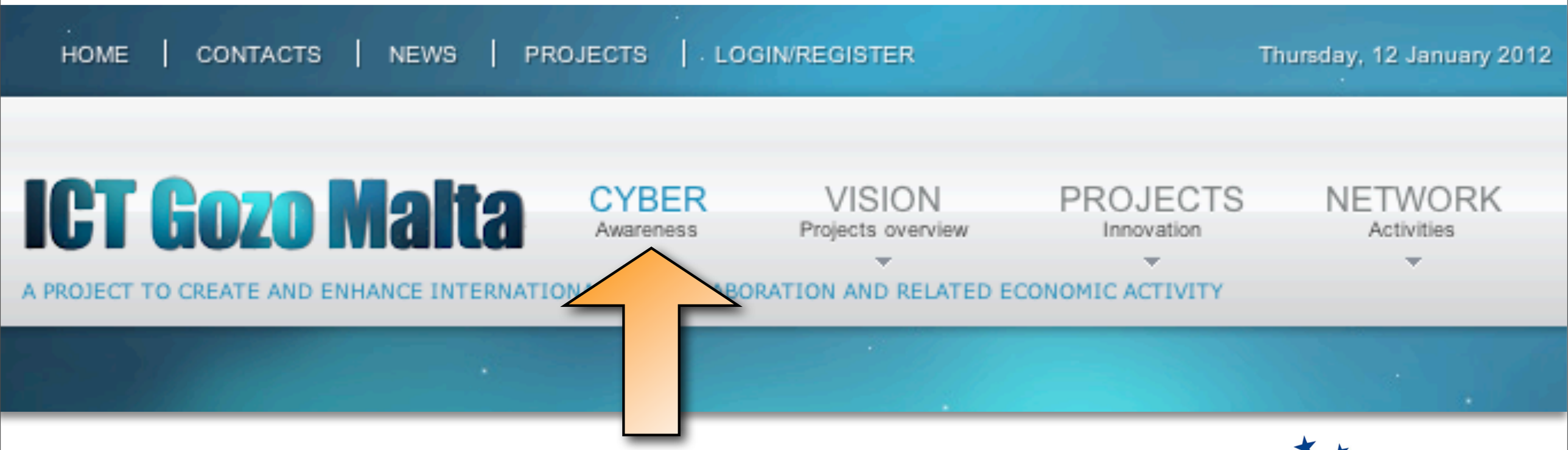
International co-operation in cyberspace: Commonwealth of Nations - 54 member nations

- **COMNET: Foundation for ICT Development**
  - **A joint initiative** of the **Government of Malta** and the **Commonwealth Secretariat**
  - Headquarters - Republic of Malta, EU
  - **Commonwealth priorities include:**
    - Improving legislation and capacity in tackling **cyber crime and other cyber space security threats**, including through the Commonwealth Internet Governance Forum's Cyber Crime Initiative
    - Commonwealth Heads of Government met in Australia, October 2011, under the theme ***'Building National Resilience, Building Global Resilience'***
      - Addressed urgent need for updating of laws with respect to cybercrime

COMNET Foundation for ICT Development

www.comnet.org.mt

National cyber awareness campaigns - examples from the ICT Gozo Malta website www.ictgozomalta.eu



GET SAFE ONLINE .org ™

be SMART ONLINE!

ins@fe

enisa European Network and Information Security Agency

STAY SMART ONLINE

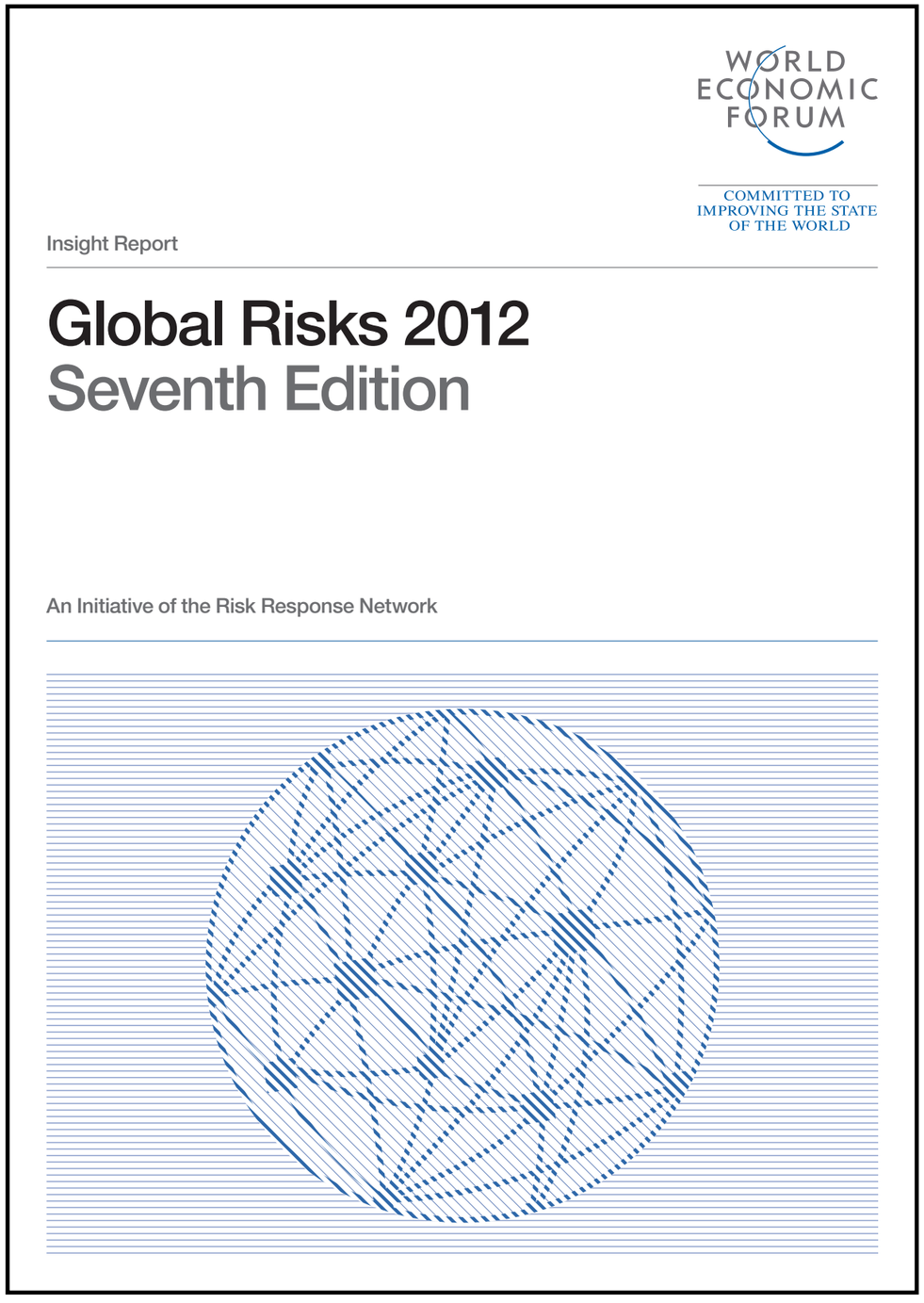
Global Perspectives on the Cyber Risk

World Economic Forum
Global Risks 2012 Report

"To provide private and public sector leaders with an independent, impartial platform to map, measure, monitor, manage and mitigate global risks." ...

"It is ... a "**call to action**" for the international community to improve current efforts"

469 experts and industry leaders contributed from all around the globe

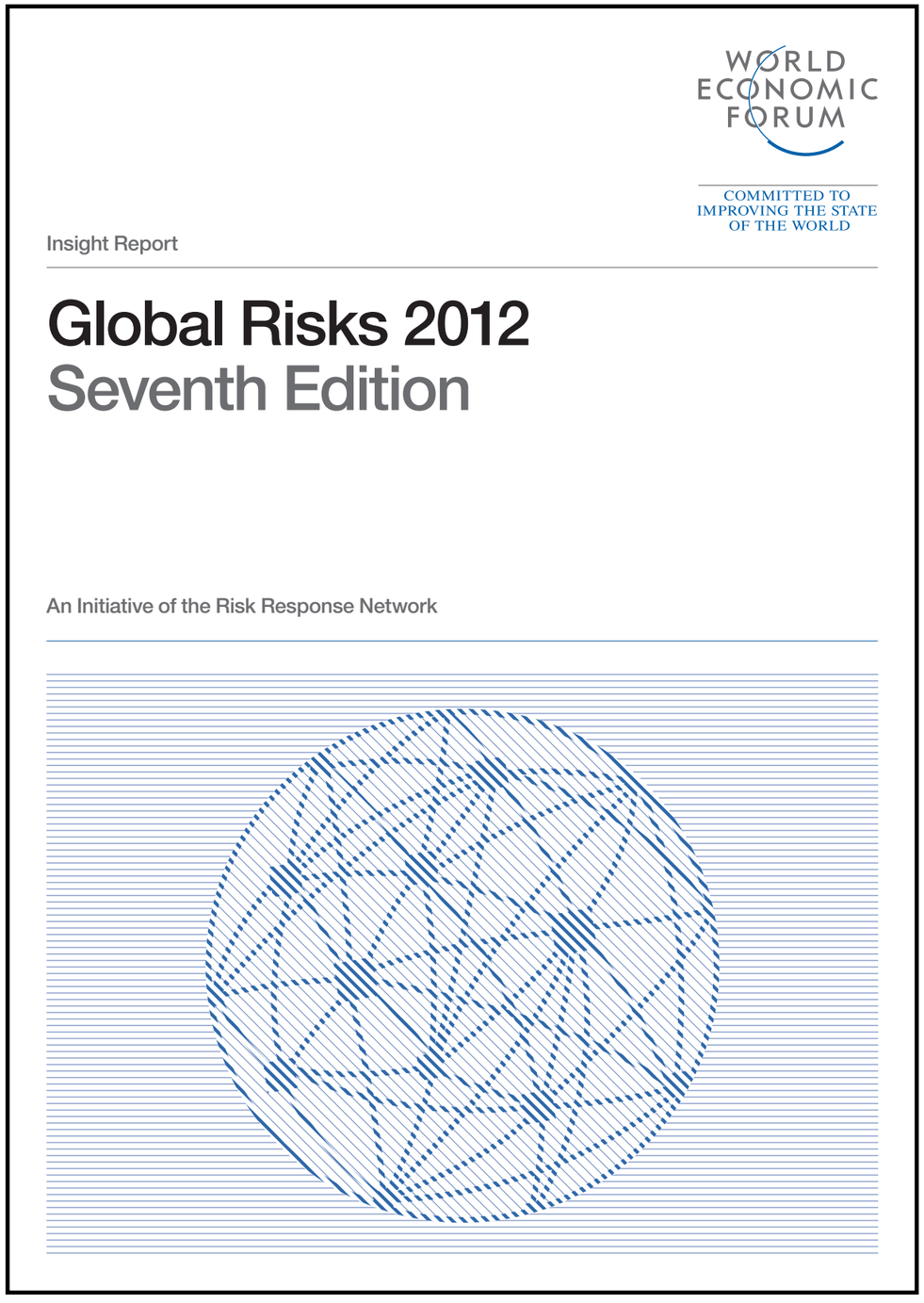


Global Perspectives on the Cyber Risk

World Economic Forum
Global Risks 2012 Report

"The more complex the system, the greater the risk of systemic breakdown, but also the greater the potential for opportunity."

"move from pure urgency-driven risk management to ... strengthening risk resilience to the benefit of global society."



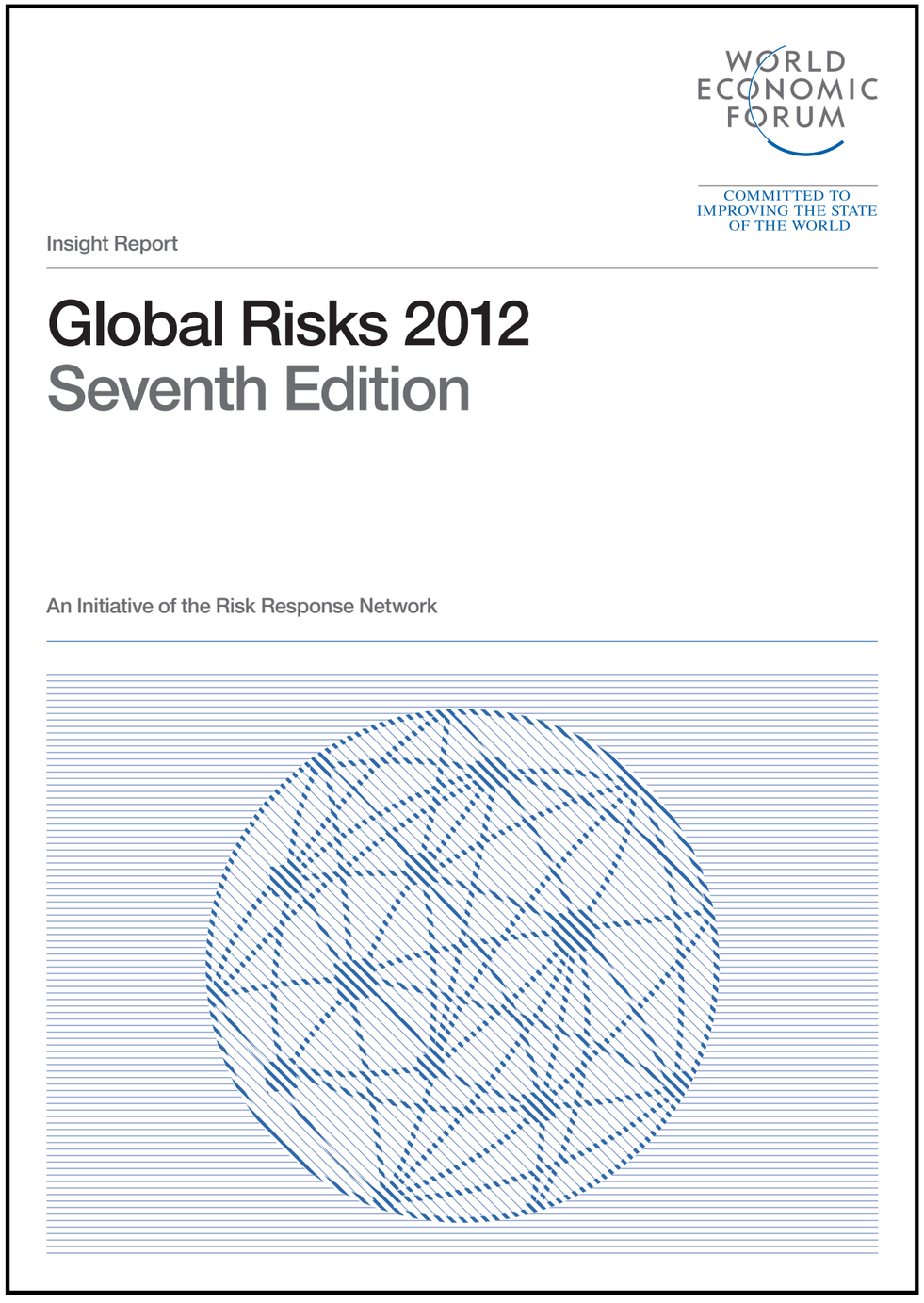
Global Perspectives on the Cyber Risk

World Economic Forum
Global Risks 2012 Report

"Only 10 years ago, the dot-com bubble burst, and claims about the Internet's potentially transformative benefits seemed to have been wildly overstated.

We can now see that they were not so much overstated as premature."

"the same could prove to be true of current alerts about the Internet's potentially transformative risks."

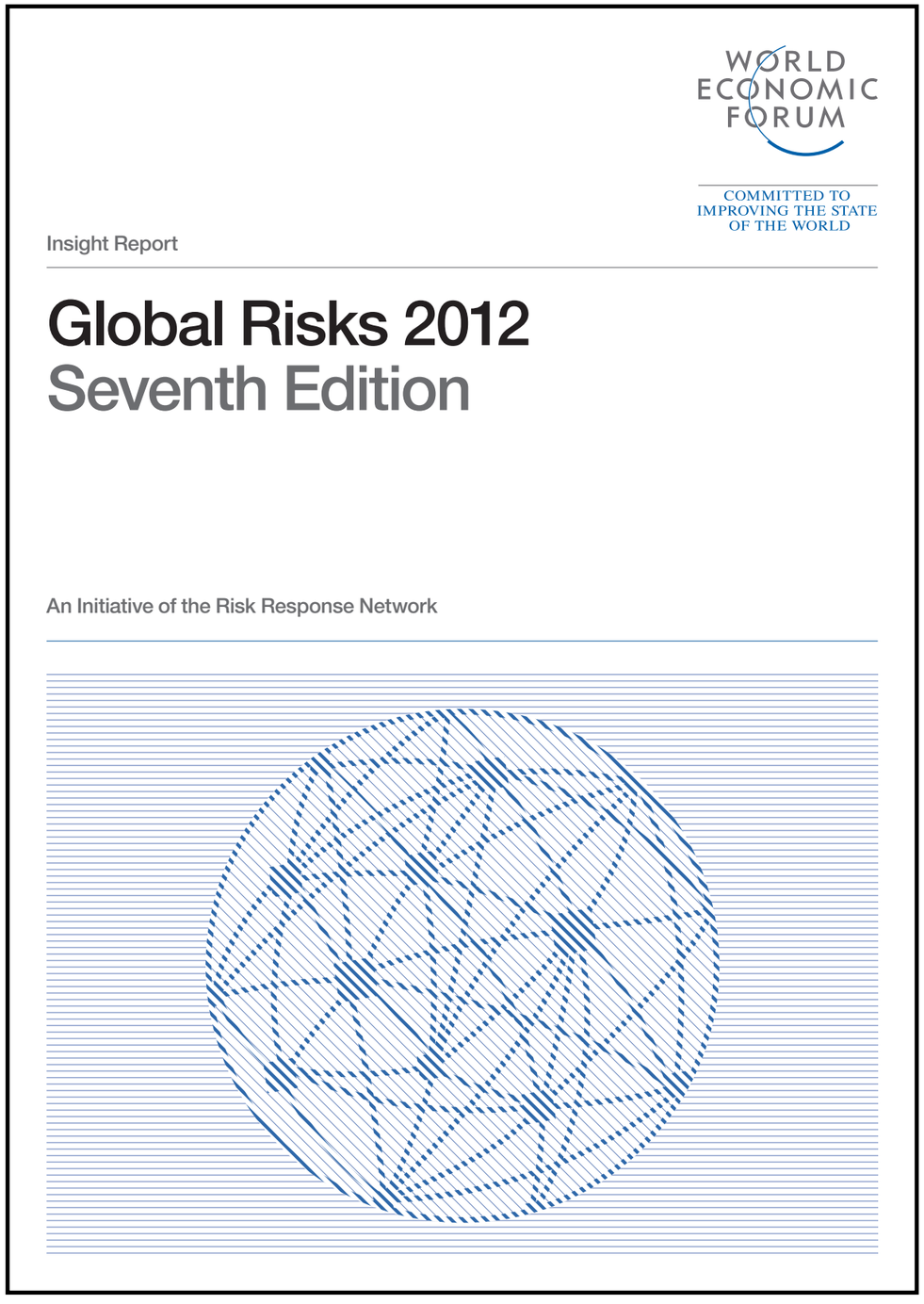


Global Perspectives on the Cyber Risk

World Economic Forum
Global Risks 2012 Report

"the costs involved in implementing safeguards, such as quality standards and risk mitigation practices, may give some individuals, firms or organizations reasons to lobby to minimize them and look for ways around them.

When losses can be passed onto others – as when banks are defined as "too big to fail" – **excessive risk-taking is likely to occur.**"



US Perspective on the Cyber Risk

The Atlantic and Government Executive's Cybersecurity Forum, Dec 2010

“My focus is on developing and delivering capabilities to protect and defend national security systems.

That really starts with the premiss that:

We have to design and architect our systems with the assumption **that adversaries, will** on occasion, **get in**.

...

There is no such thing really as secure anymore.”

Debora Plunkett
Director of the Information Assurance Directorate (IAD)
U.S. National Security Agency

US Perspective on the Cyber Risk

The Atlantic and Government Executive's Cybersecurity Forum, Dec 2010

"We have to be really careful that we don't make it to easy for the adversary, so we have to make them work harder.

We [ed: the United States] can't misplace our trust in different components of the system that might have **already been violated**.

We have to again assume that all components of our system are not safe, and **make sure we are adjusting accordingly.**"

Debora Plunkett
Director of the Information Assurance Directorate (IAD)
U.S. National Security Agency

US Perspective on the Cyber Risk

"Insider Threats. Insiders have caused significant damage to US interests from the theft and unauthorized disclosure of classified, economic, and proprietary information and other acts of espionage.

We assess that trusted insiders using their access for malicious intent **represent one of today's primary threats to US classified networks."**

Unclassified Statement for the Record on the

Worldwide Threat Assessment of the

US Intelligence Community for the

House Permanent Select Committee on Intelligence

James R. Clapper

Director of National Intelligence

February 2, 2012

US Perspective on the Cyber Risk

"We judge that evolving business practices and information technology will provide even more opportunities for FIS (foreign intelligence services), trusted insiders, hackers, and others to collect sensitive US economic data.

Corporate supply chains and financial networks will increasingly rely on global links that can be exploited by foreign collectors, and the growing use of cloud data processing and storage may present new challenges to the security and integrity of sensitive information.

Unclassified Statement for the Record on the

Worldwide Threat Assessment of the

US Intelligence Community for the

House Permanent Select Committee on Intelligence

James R. Clapper

Director of National Intelligence

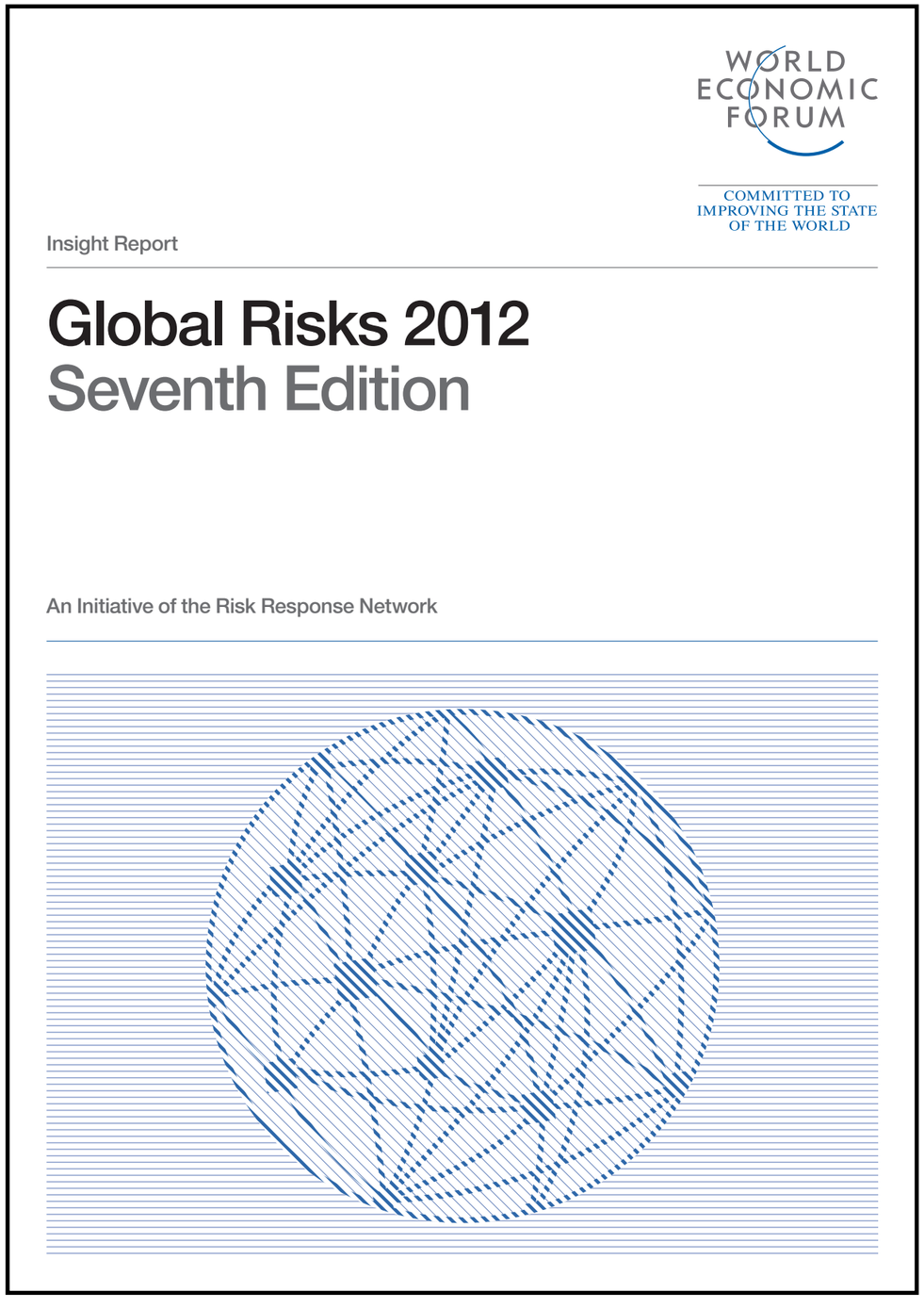
February 2, 2012

Global Perspectives on the Cyber Risk

World Economic Forum
Global Risks 2012 Report

"How can businesses and governments **prevent a rapid breakdown in trust** following the emergence of a new widespread risk?"

"How can leaders **break the pattern** of crises followed by reactionary regulation and develop anticipatory and holistic approaches to system safeguards?"



Industry Must Demand / Lead the Drive for a Trustworthy and Dependable Computing Ecosystem that Holistically Converges Safety and Security Capabilities

Synaptic Labs' Annual Report on the Global Cyber Security Status 2012

1. High level overview
2. Global assessments and global responses
3. **The stability of Nations is at risk**
4. Our cyber defences are very low
5. Experts: The cyber risk is not overstated
6. Closing statement
7. Related videos

The stability of nations is at risk

UK Government Position
2010, 2011, 2012

The UK's critical infrastructure faces a **"real and credible" threat** of cyber attack

"It goes to the heart of our economic well-being and national interest."

- **Iain Lobban**
  Director General,
  UK Gov. Communications Headquarters (GCHQ)

Companies are carrying far too much risk!

UK Government: We must protect cyberspace

UK Government Position
Cyber Security Strategy 2011

We must take forward leaning action to address the cyber threats:

- "Alongside our existing defence and security capabilities, **the UK must be capable of protecting our national interests in cyberspace.**"

Recall that the international consensus is:

Collaborative corrective action must be taken NOW by all sectors to:

1. Maintain **public confidence** in existing ICT enabled systems
2. **Support the uptake of future ICT enabled advances such as cloud computing that promise massive societal benefits**

“The trustworthiness of our increasingly digitised world is at stake.”

EU Commission funded FP7 RISEPTIS Report

UK Government: We must protect cyberspace

UK Government Position
Cyber Security Strategy 2011

"Any reduction in trust towards online communications can now cause serious economic and social harm to the UK."

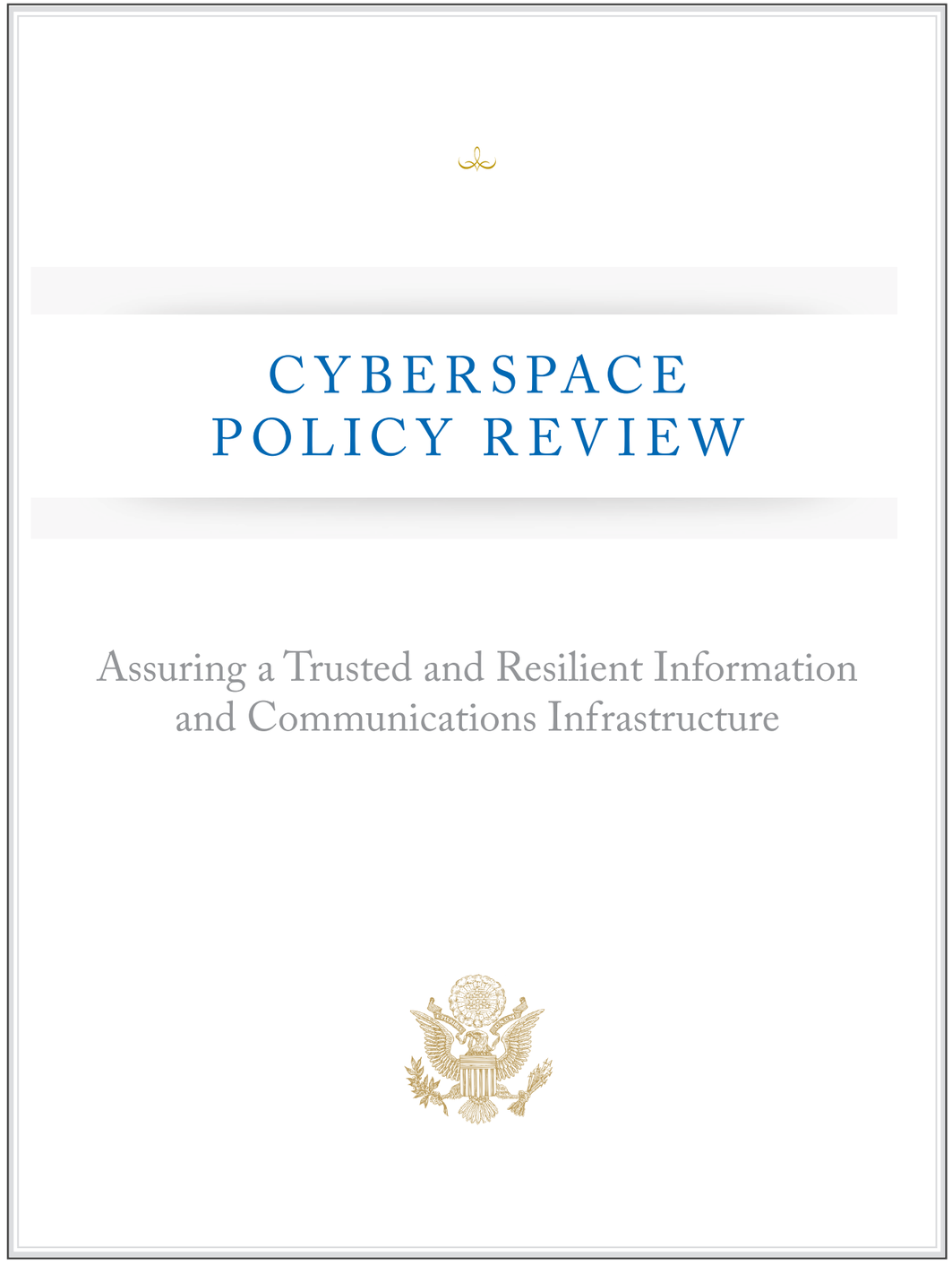
The stability of nations is at risk

US Government Position
Cyberspace Policy Review

“failure to protect cyberspace is one of the most urgent national security problems”

“cybersecurity risks pose some of the most serious economic and national security challenges of the 21st Century.”

“... a growing array of state and non-state actors **are** compromising, stealing, changing, or destroying information and could cause critical disruptions to U.S. systems”



Introducing the Security & Defence Agenda

- Brussels' only specialist security and defence think-tank
- Wholly independent (10th anniversary)
- Brings together experts and policymakers from:
  - the EU institutions
  - NATO
  - national governments
  - industry
  - the media
  - think-tanks
  - academia and NGOs

SDA

SECURITY & DEFENCE AGENDA

Global Perspectives on the Cyber Risk

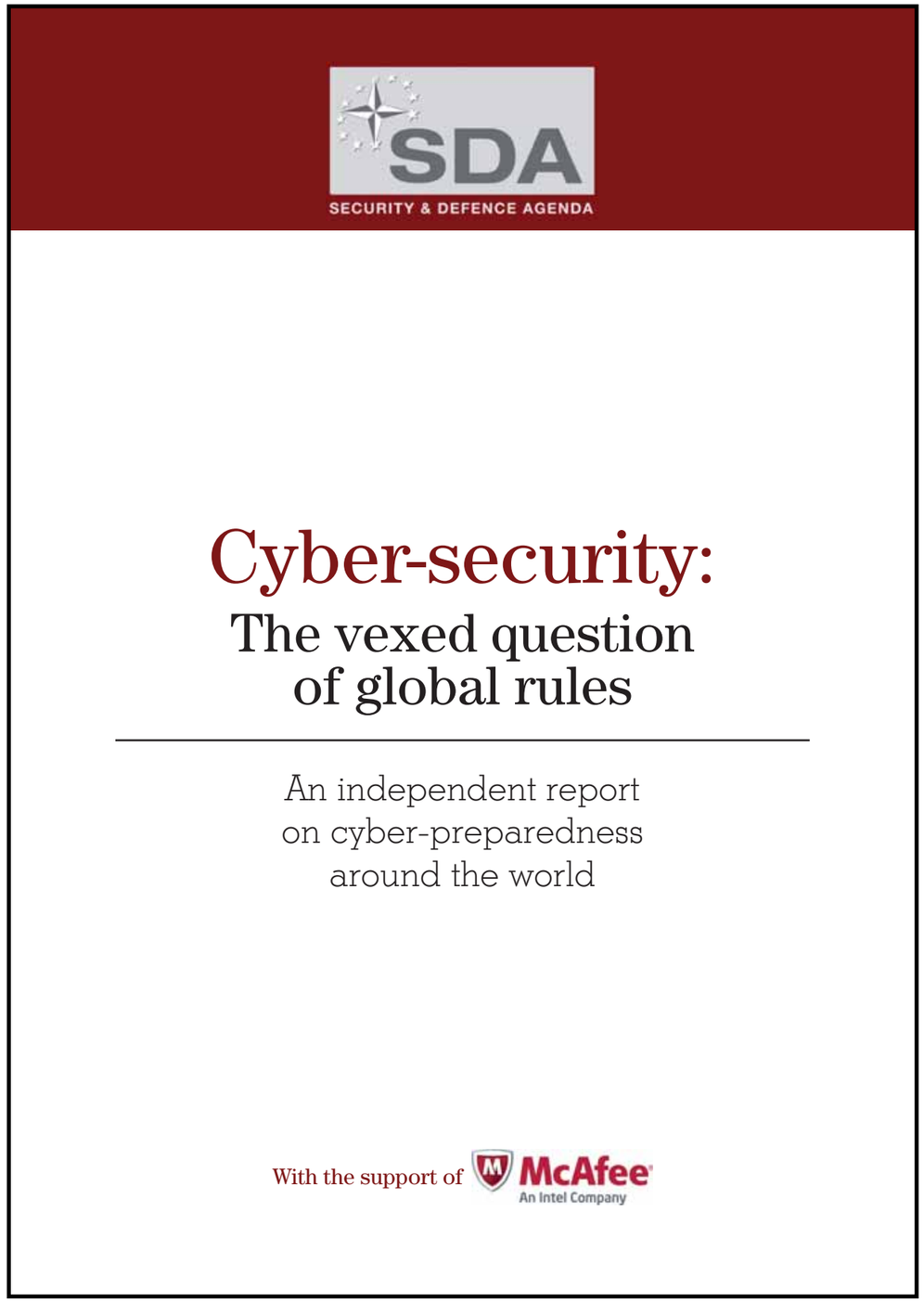
Security & Defence Agenda
Cyber-Security 2012 Report

"Offers a global snapshot of current thinking about the cyber-threat."

Based on interviews with **80 policy makers and cyber security experts** in government, business and academia **across 27 countries**

and

anonymous surveys of 250 world leaders in 35 countries

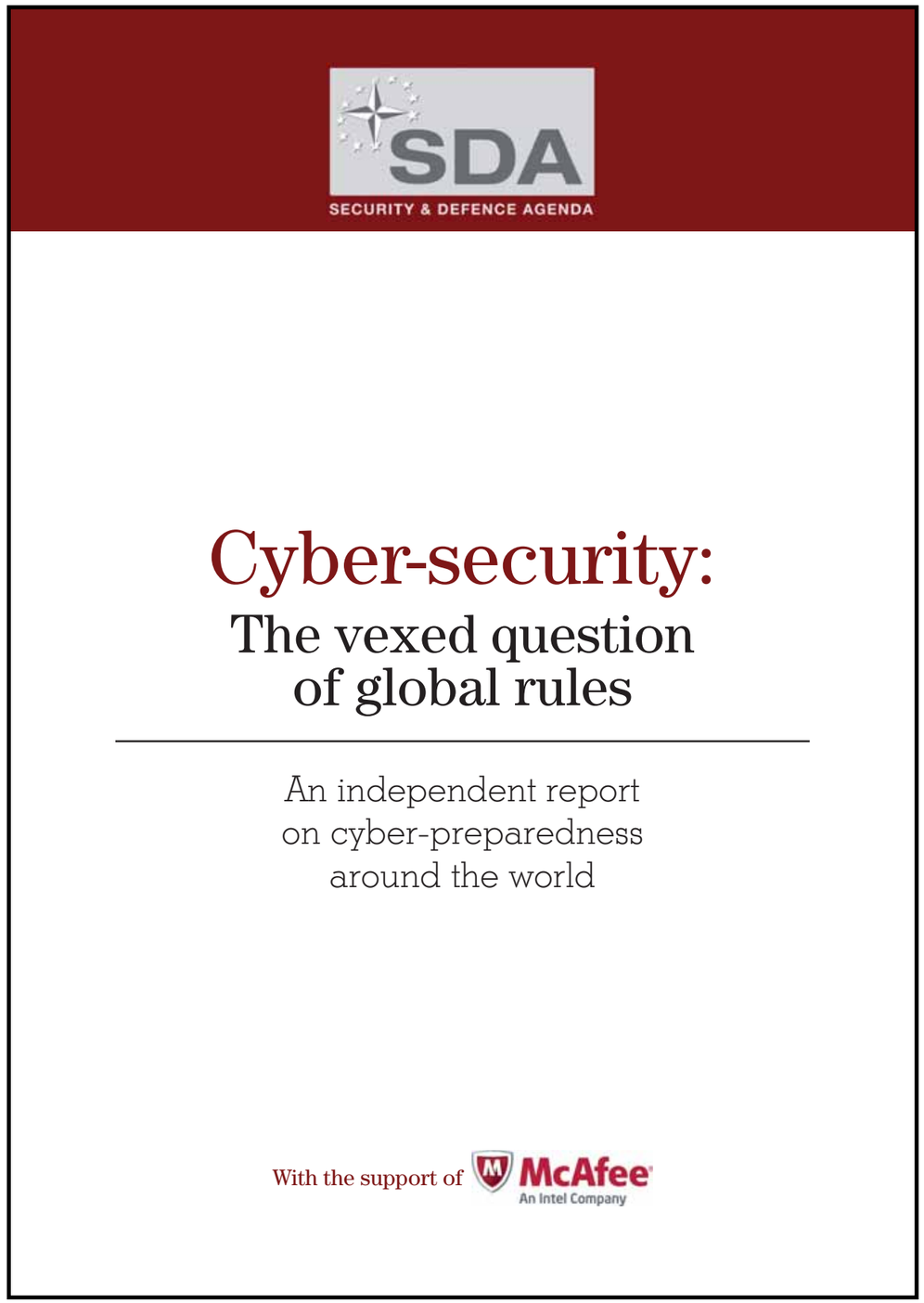


Global Perspectives on the Cyber Risk

Security & Defence Agenda
Cyber-Security 2012 Report

"Damage or disruption to critical infrastructure is seen as the greatest single threat posed by cyber-attacks"

"a national threat with wide economic consequences."



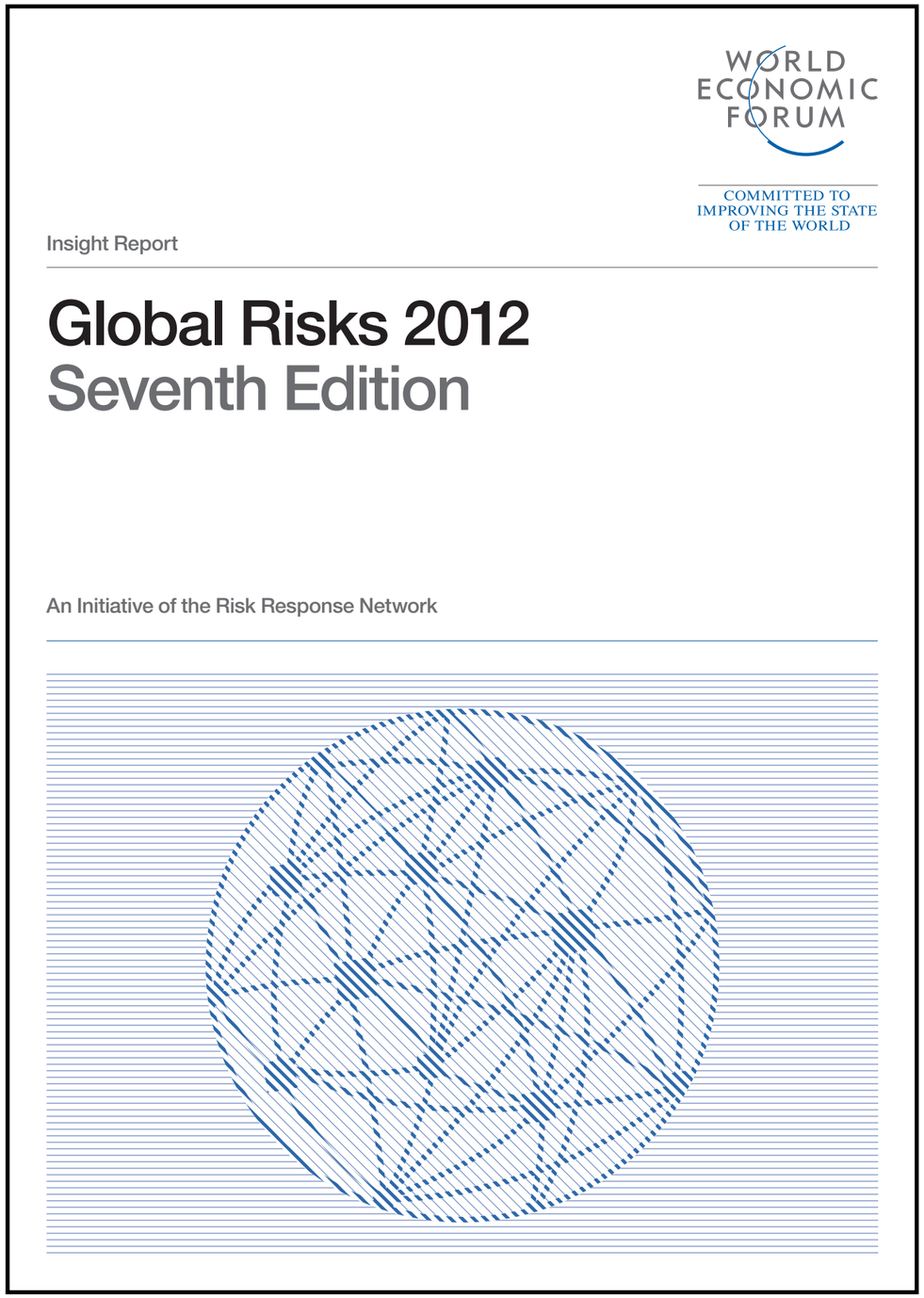
Cyber attacks leading to critical systems failure

World Economic Forum
Global Risks 2012 Report

- **Critical systems failure occurs when a single failure triggers cascading failures** in the critical infrastructure and networks

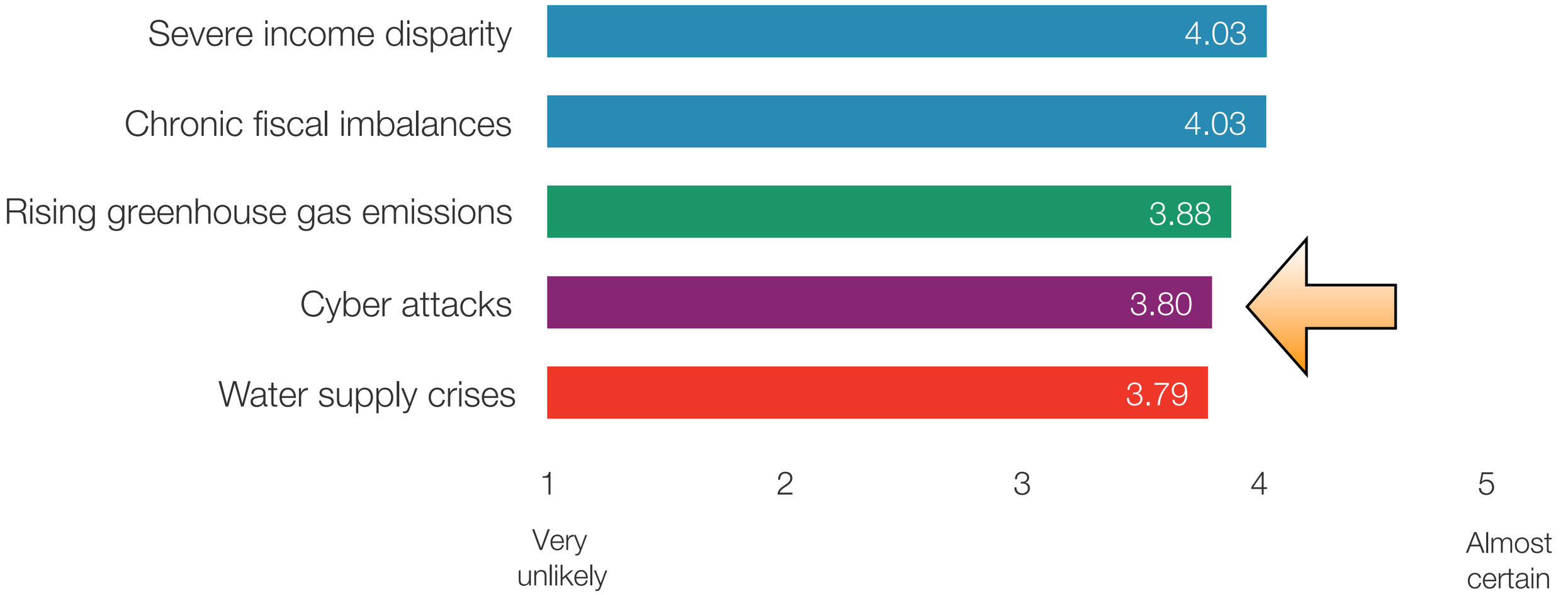
- **Critical systems failure identified as "a key concern for world leaders from government, business and civil society."**

- **Critical systems failure will "most likely be caused by cyber attacks"**



Cyber attacks rank 4th out of 50 global risks

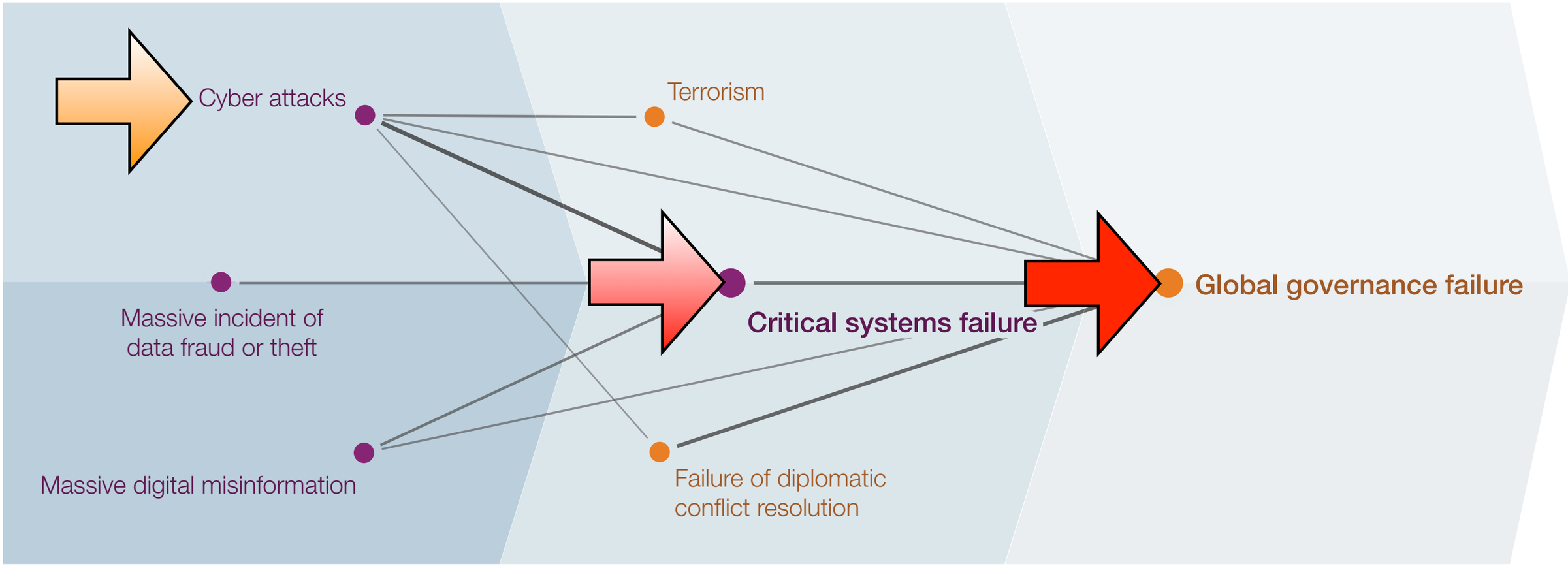
World Economic Forum
Global Risks 2012 Report



Cyber attacks: State-sponsored, state-affiliated, criminal or terrorist

Cyber attacks identified as most likely cause of global governance failure

World Economic Forum
Global Risks 2012 Report

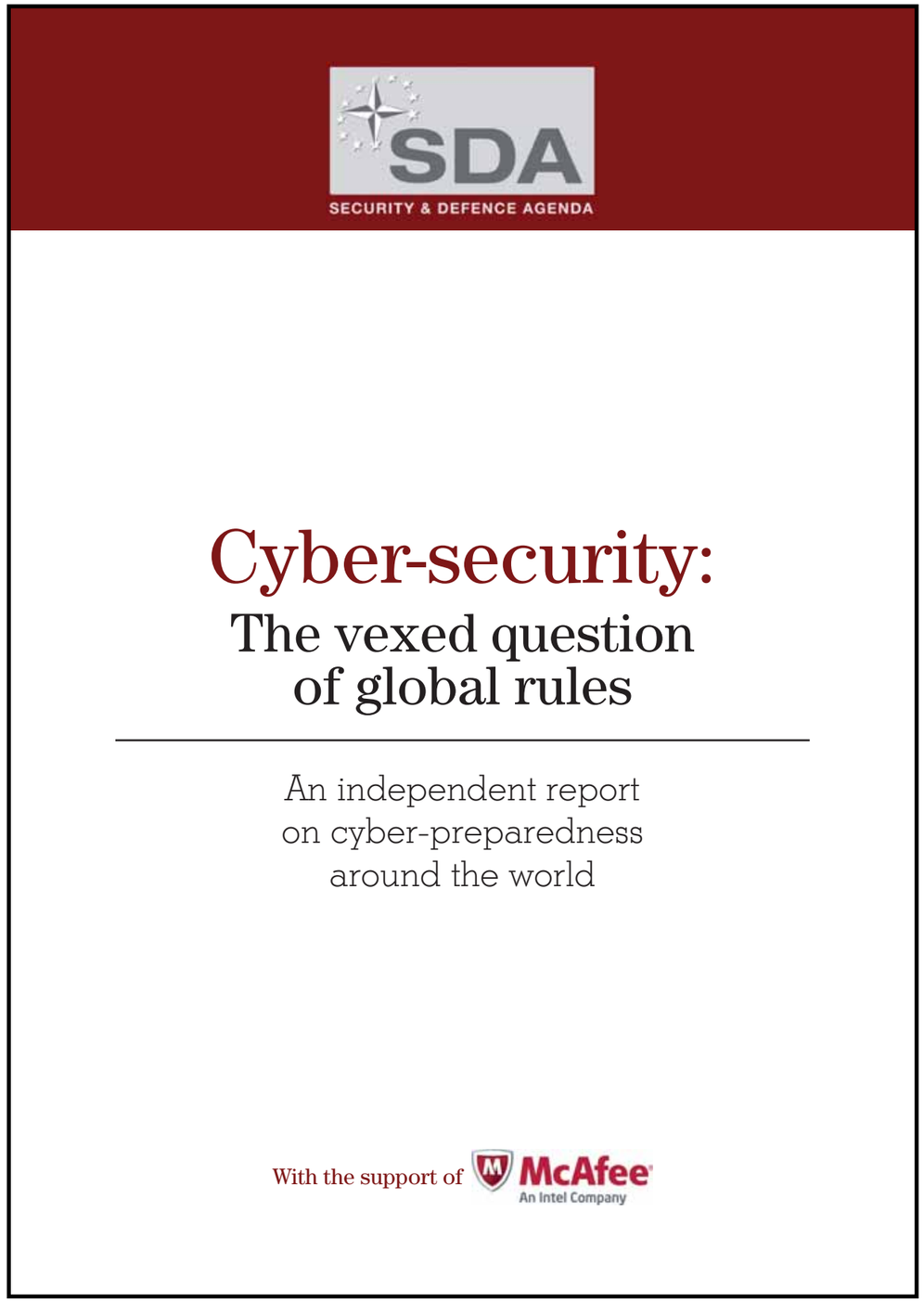


Global Perspectives on the Cyber Risk

Security & Defence Agenda
Cyber-Security 2012 Report

Survey of 250 world leaders in 35 countries:

- **57% believe a cyber arms race is taking place**
- **74% believe that cyber defence is** as important or **more important than missile defence**
- **84% see cyber-attacks as a threat to national and international security and to trade**

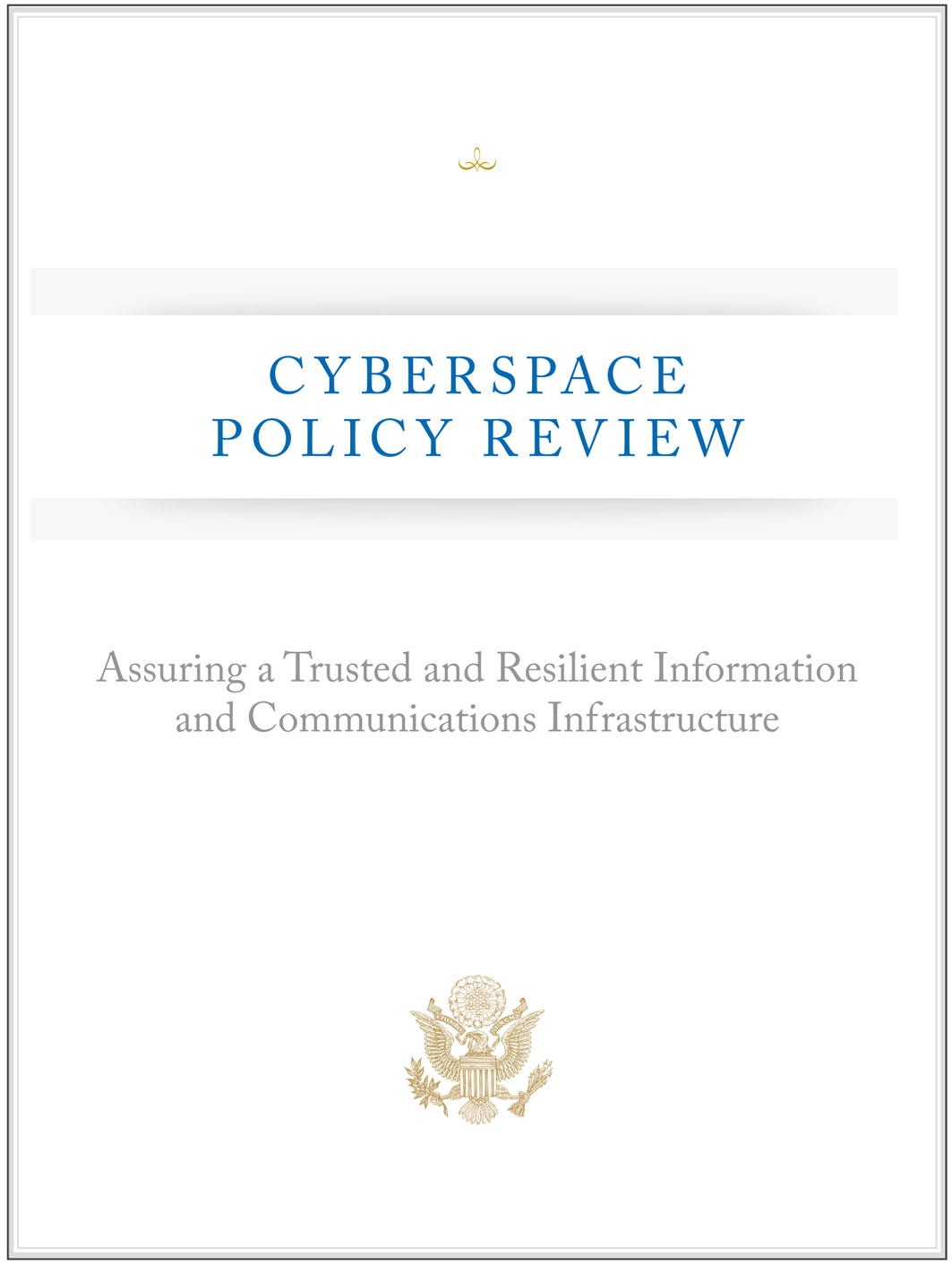


The stability of nations is at risk

US Government Position
Cyberspace Policy Review

"**connectivity between** information **systems,** the Internet, and other infrastructures **creates opportunities for attackers to disrupt** telecommunications, electrical power, energy pipelines, refineries, financial networks, and other **critical infrastructures.**"

"a number of nations already have the technical capability to conduct such attacks."


CYBERSPACE POLICY REVIEW

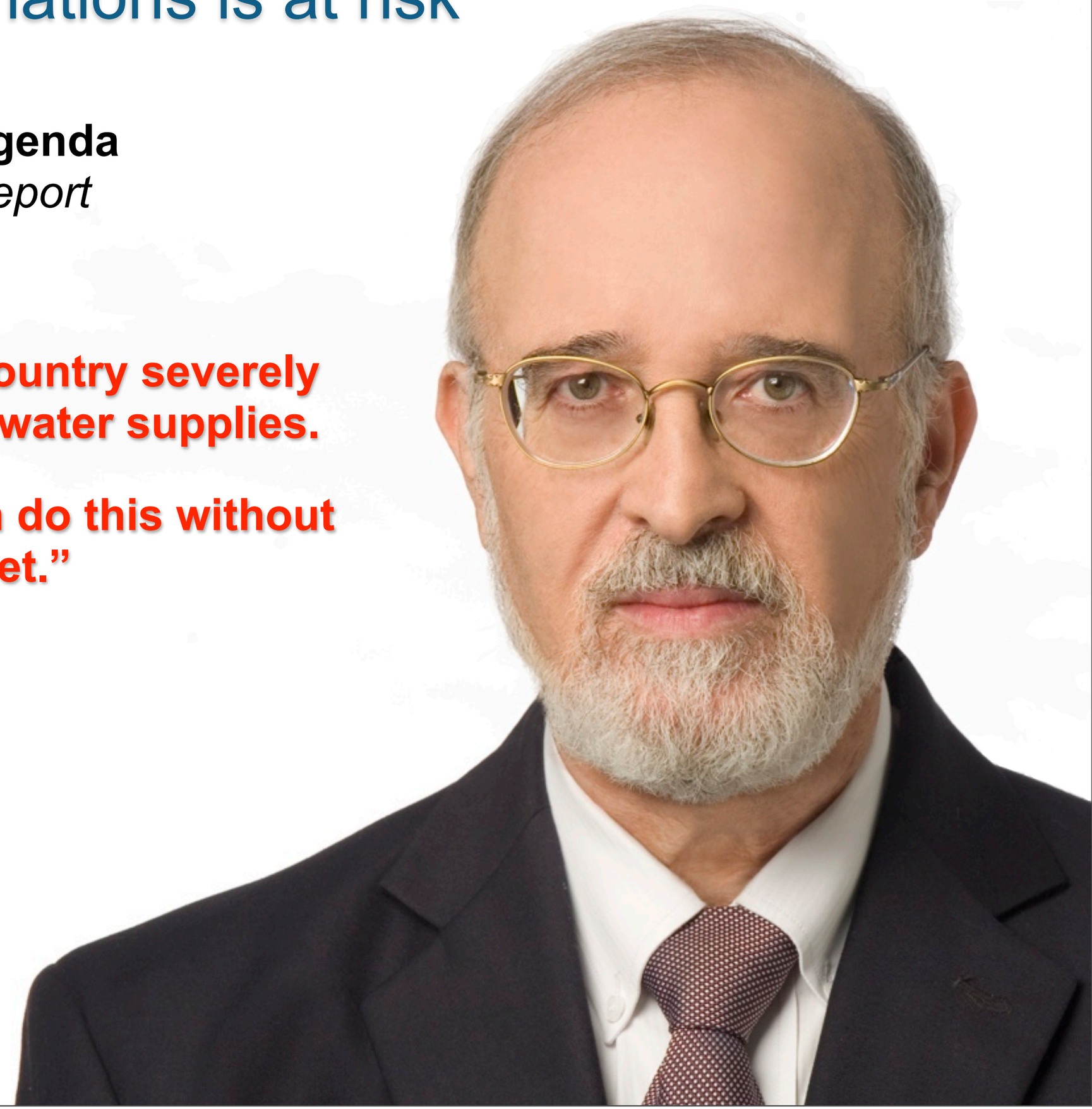
Assuring a Trusted and Resilient Information and Communications Infrastructure

The stability of nations is at risk

Security & Defence Agenda
Cyber-Security 2012 Report

"If you want to hit a country severely you hit its power and water supplies.

Cyber technology can do this without shooting a single bullet."



Prof. Isaac Ben-Israel
Cyber Security advisor to
Israel Prime Minister
Director of Defense R&D
Directorate in Israel
Ministry of Defense
(1998-)

The stability of nations is at risk

“We are a nation unprepared to properly defend ourselves and recover from a strategic cyber attack.”

- **An attack could bring down the electricity grid for 6 months**
- No communications, no banking, food production ceasing
- It would require months to bring the country back online

– **O. Sami Saydjari’s**
Testimony to Congress

President and Founder, Cyber Defense Agency
Formerly Director’s Fellow, **National Security Agency** and Program Manager, Information Assurance, **Defense Advanced Research Projects Agency**

The stability of nations is at risk

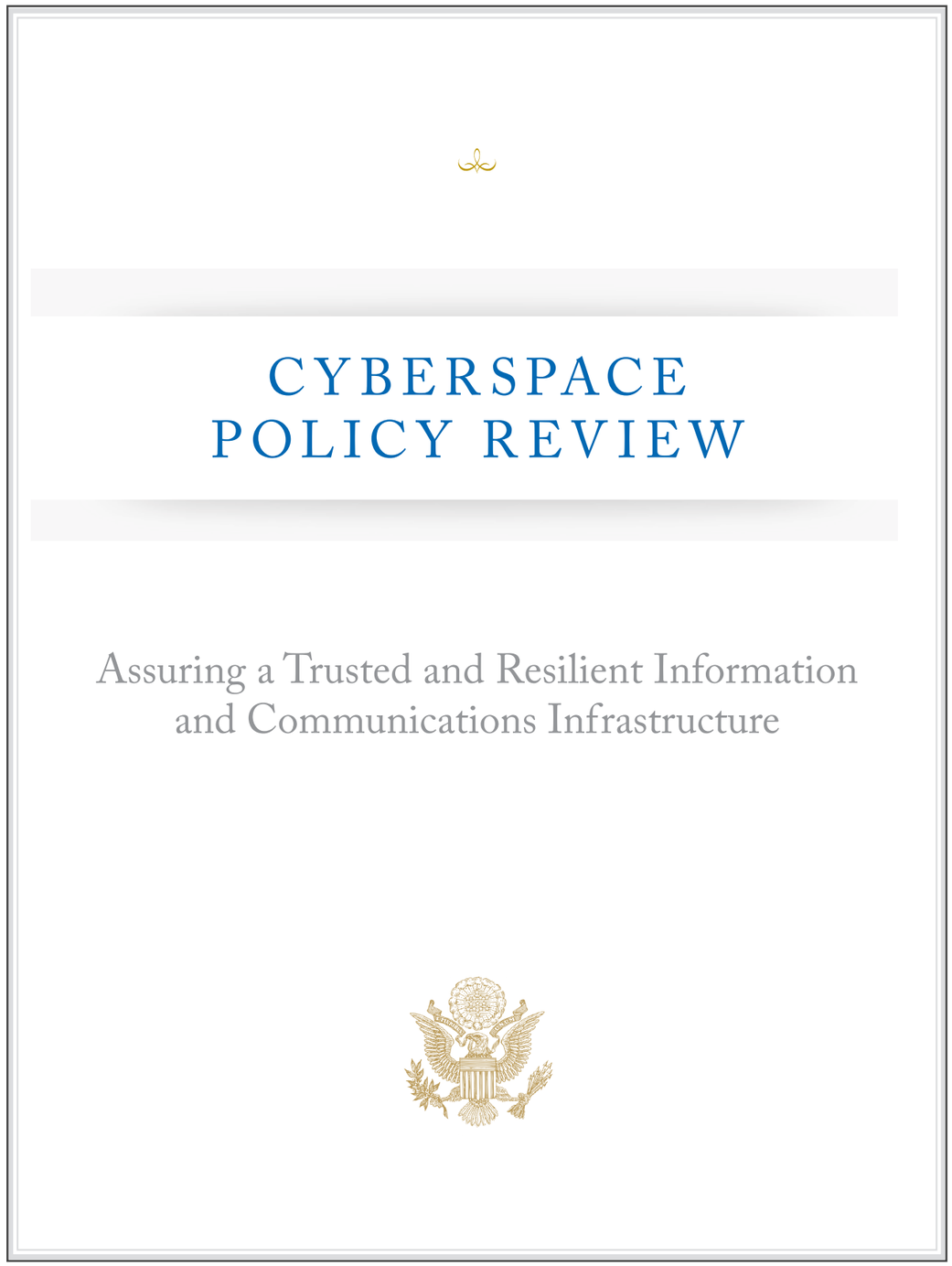
US Government Position
Cyberspace Policy Review

"our defense and military networks are under constant attack. [ed. 15,000 a day] This status quo is no longer acceptable – not when there's so much at stake.

We can and we must do better.

Given the **enormous damage** that can be caused by even a single cyber attack, ad hoc responses will not do.

[It is not] sufficient to simply strengthen our defences after incidents or attacks occur."

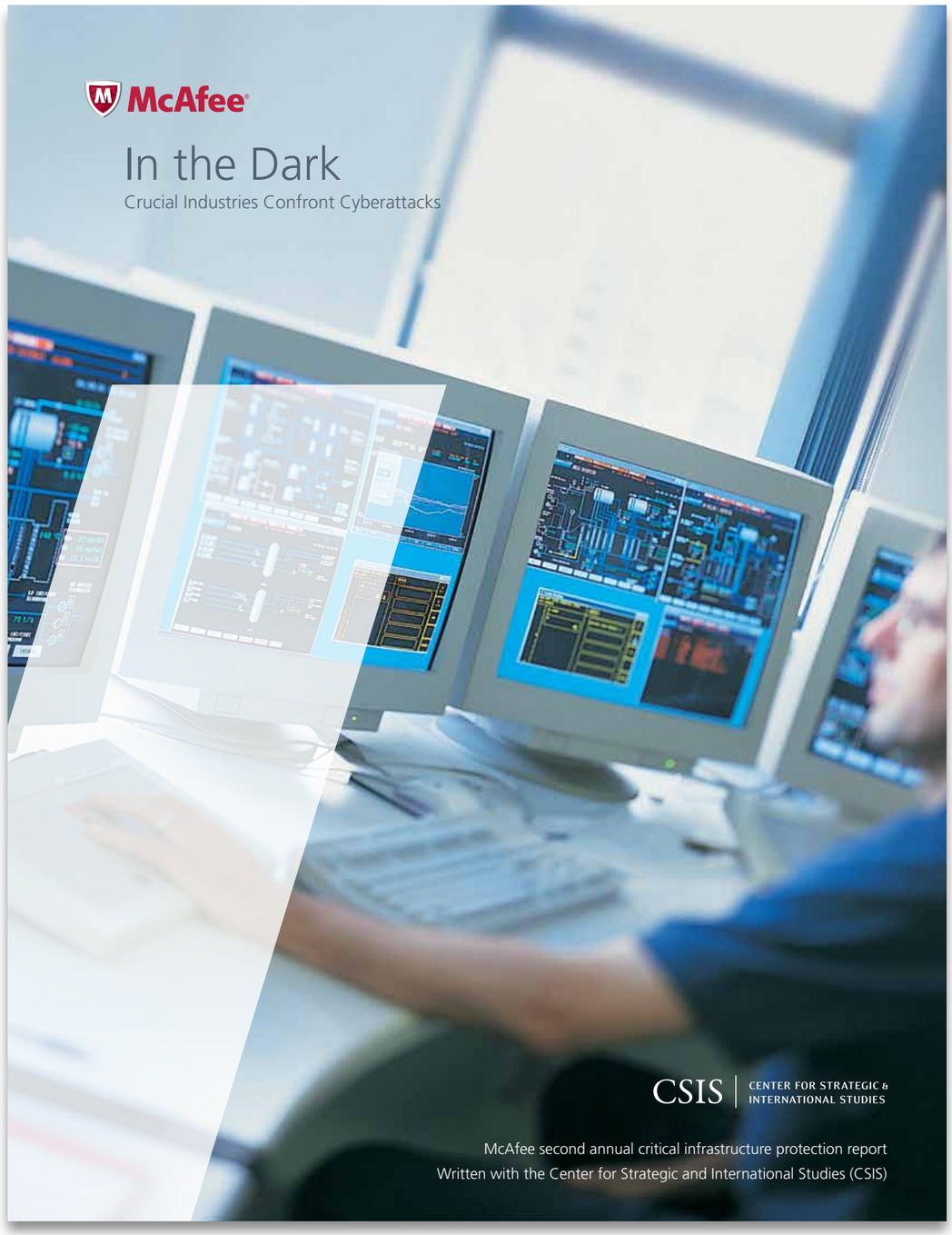


The stability of nations is at risk

McAfee and CSIS
2nd Annual Critical Infrastructure Protection Report, **March 2011**

In the Dark
Crucial Industries Confront Cyberattacks

"Nearly two-thirds of critical infrastructure companies report regularly finding malware designed to sabotage their systems."



www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf

Synaptic Labs' Annual Report on the Global Cyber Security Status 2012

1. High level overview
2. Global assessments and global responses
3. The stability of Nations is at risk
4. **Our cyber defences are very low**
5. Experts: The cyber risk is not overstated
6. Closing statement
7. Related videos

ICT Gozo Malta

www.ictgozomalta.eu

Malta International
Cyber Awareness Seminar

November 2011

"Our Security Status is Grim"

(and the way ahead will be hard)

Brian Snow

Former Technical Director
Information Assurance Directorate
United Sates National Security Agency

The stability of nations is at risk

"Today's Trust Bubble products are rife with a huge pile of crippling un-addressed conceptual and implementation debt.
That is a one-two punch. And as were the Credit Derivative products in 2007, widely used, little understood, and less analyzed!

I said in March 2010 at the RSA Conference that **we are ripe for a Trust Bubble melt-down with the same scale of consequences that the Credit Markets suffered**.

I predicted that it COULD (not WOULD) happen within 3-5 years, possibly even within 18 months…"

Brian Snow
Our Security Status is Grim
Former US NSA, 35 years incl. Technical Director (R&D, IAD, ADET)

The stability of nations is at risk

"I now feel we may have only long weeks to short months before **we COULD feel even greater pain from the immense pile of "debt"** (both conceptual and technical) **that security vendors are carrying**.

Please realize, we are in desperate trouble!

We have to dig out of this, or **else the world economy is headed for a severe crash!**

We are moving at a snail's pace against an avalanche of MALICE.

It is insane not to act!"

Brian Snow
Our Security Status is Grim
Former US NSA, 35 years incl.
Technical Director (R&D, IAD, ADET)

The stability of nations is at risk

“I am here to tell you that
your cyber systems continue to function and serve you

NOT due to the EXPERTISE of your security staff,

but

solely due to the SUFFERANCE of your opponents.”

November 2011

Brian Snow
Our Security Status is Grim
Former US NSA, 35 years incl.
Technical Director (R&D, IAD, ADET)

How **LOW** are our cyber security defences?

U.S. Government Position
U.S. National Security Agency

"There is no such thing as secure any more."

– **Debora Plunkett**
Director
Information Assurance Directorate
U.S. National Security Agency

Introduction to Melissa Hathaway

- Formerly:
  - Senior Advisor to the Director of National Intelligence
  - Contributed to the development of the Comprehensive National Cybersecurity Initiative (CNCI)
  - Appointed the Director of the Joint Interagency Cyber Task Force (JIACTF)
  - Secialized in cybersecurity strategies with consulting firm Booz Allen Hamilton, focusing on leading the information operations and long-range strategy and policy support business units
  - Led the US Cyber Space Policy Review

Melissa Hathaway
Led U.S. President Obama's Cyberspace Policy Review

(video used with permission)

Assessment by Melissa Hathaway May 2010

Speaking at the U.S. Oak Ridge National Laboratory CSIIRW 2010 event

"I think it is unconscionable that our leaders are not talking about what is really happening

and some of it is because of **the fear that we are going to lose trust in the core infrastructure**

and/or that we are going to lose public confidence."

Melissa Hathaway
Led U.S. President Obama's Cyberspace Policy Review

(video used with permission)

Delays in reporting attacks

- Hacks against NASA managed satellites reported up to 4 years later

- DigiNotar failed to immediately notify the Dutch Government of their breaches

- Hacks in the Verisign corporate network occurred in 2010

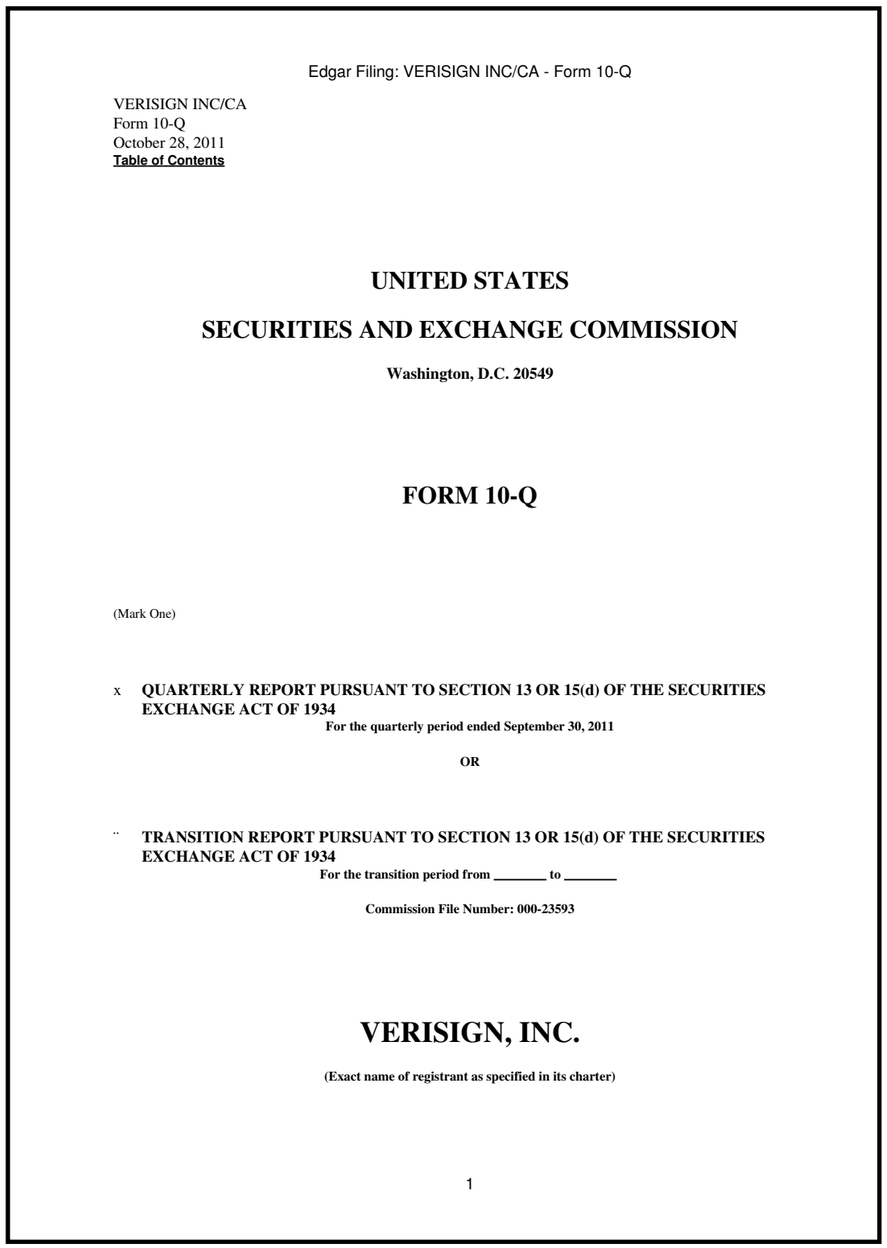
  Management was informed of the incidents in September 2011

The level of risk is declared: VeriSign's Form 10-Q Quarterly Report SEC filing October 2011 (p.33)

"In 2010, **the Company faced several successful attacks** … **Information ... was exfiltrated**.

... we **cannot assure** that our remedial actions will be sufficient to thwart future attacks or prevent the future loss of information.

... although the Company is unaware of any situation in which possibly exfiltrated information has been used, **we are unable to assure that such information was not or could not be used in the future."**



Edgar Filing: VERISIGN INC/CA - Form 10-Q

VERISIGN INC/CA
Form 10-Q
October 28, 2011
Table of Contents

UNITED STATES

SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

FORM 10-Q

(Mark One)

x **QUARTERLY REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**
For the quarterly period ended September 30, 2011

OR

¨ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**
For the transition period from _____ to _____

Commission File Number: 000-23593

VERISIGN, INC.

(Exact name of registrant as specified in its charter)

1

SYNAPTIC LABORATORIES LTD.

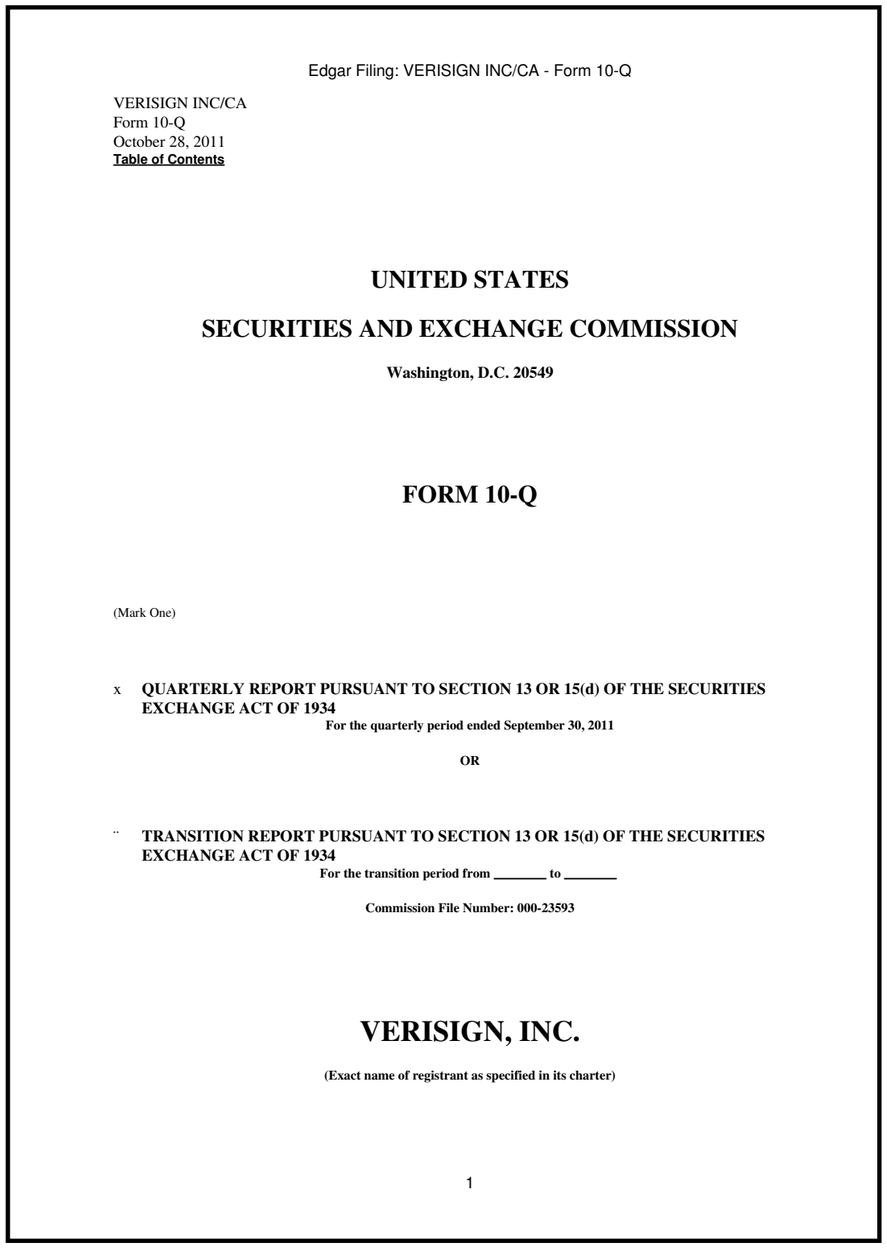
4. Our (business) cyber defences are very low

The level of risk is declared: VeriSign's Form 10-Q Quarterly Report SEC filing October 2011 (p.33)

"It is critical to our business strategy that our facilities and infrastructure remain secure and are perceived by the marketplace to be secure.

The Company as an operator of critical infrastructure is frequently targeted and experiences a high rate of attacks.

These include the most sophisticated form of attacks, ... **attacks virtually impossible to anticipate and defend against."**



Edgar Filing: VERISIGN INC/CA - Form 10-Q

VERISIGN INC/CA
Form 10-Q
October 28, 2011
Table of Contents

UNITED STATES

SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

FORM 10-Q

(Mark One)

x **QUARTERLY REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**
For the quarterly period ended September 30, 2011

OR

¨ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**
For the transition period from _____ to _____

Commission File Number: 000-23593

VERISIGN, INC.

(Exact name of registrant as specified in its charter)

1

Assessment by Melissa Hathaway May 2010

"In director [ed. of US National Intelligence] Blair's testimony to the Senate in February, he stated:

'The national security of the United States, our economic prosperity, and daily functioning of our Government is dependent on a dynamic public and private information infrastructure, and **that it's threatened.**'

And I would say that it is compromised.

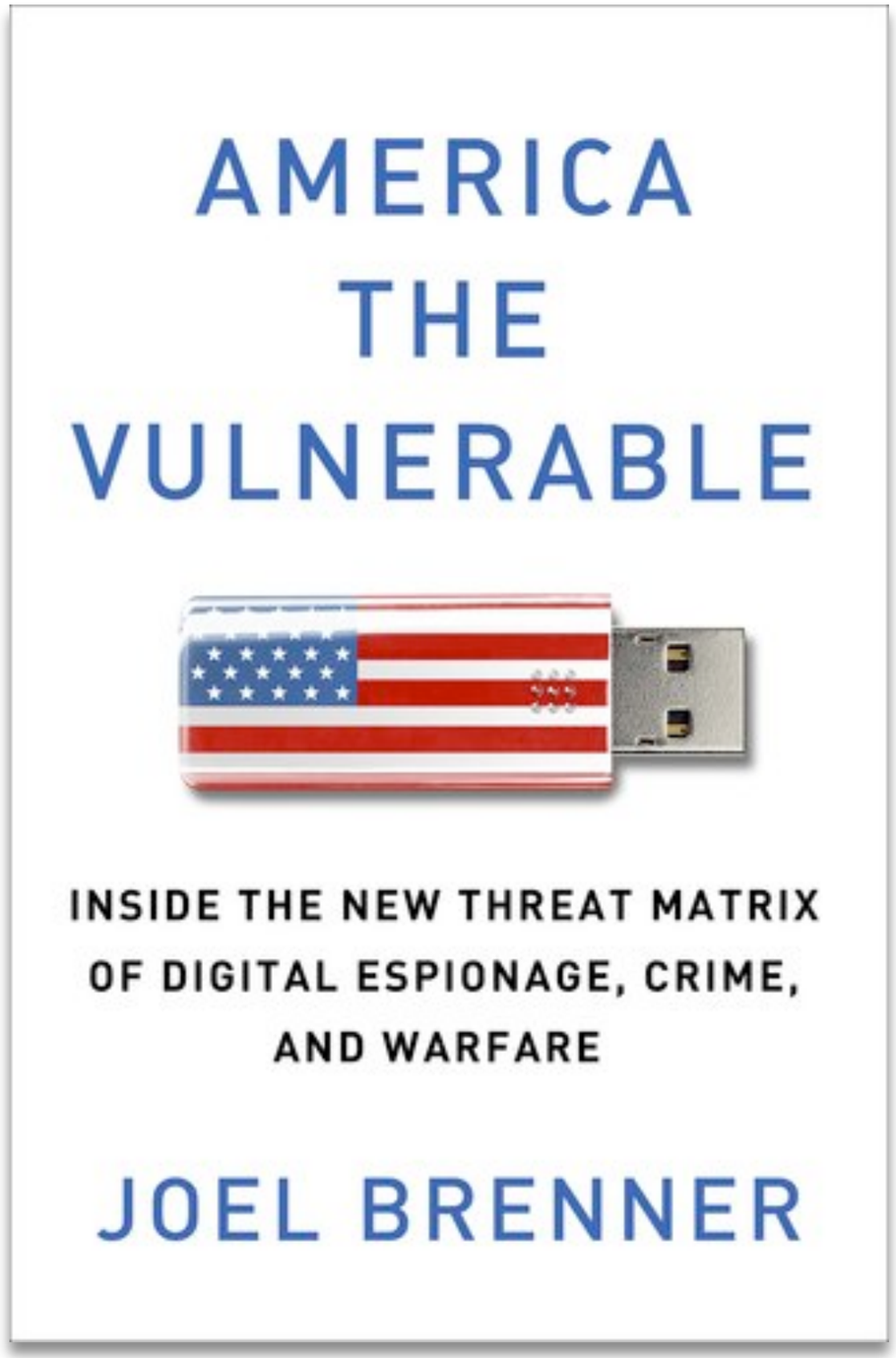
It's been compromised already."

Melissa Hathaway
Led U.S. President Obama's Cyberspace Policy Review

(video used with permission)

Assessment by Joel Brenner September 2011

Image: by Jodi Cobb



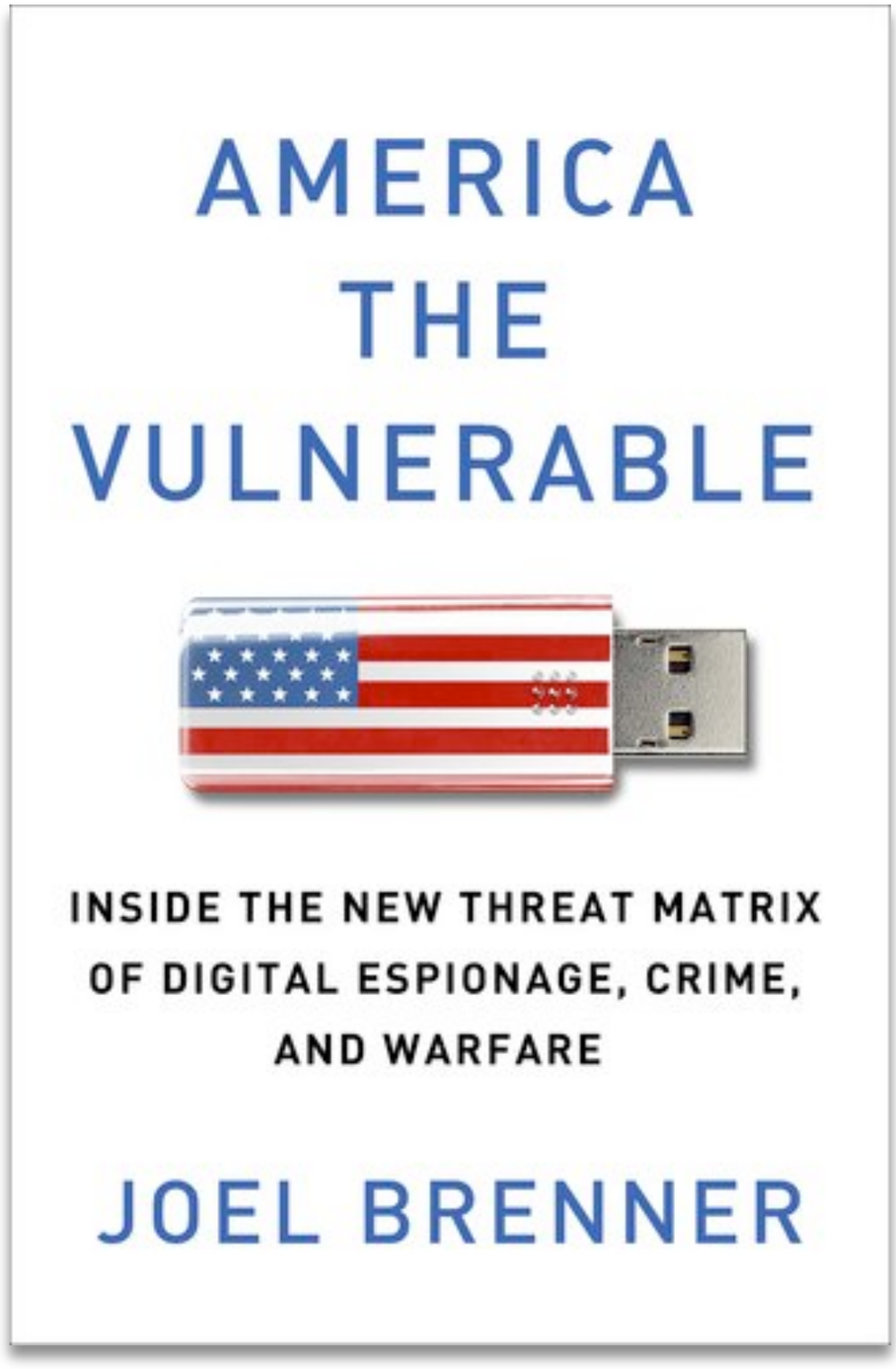
"I spent most of the first decade of the 21'st century **working at the heart of the U.S. Government's efforts** to thwart spying and terrorism against us, first as inspector general of the NSA, and then as chief of counter-intelligence for the director of National Intelligence."

Assessment by Joel Brenner September 2011

"The truth I saw was brutal and intense: Electronic thieves are stripping us blind."

"Technologies that cost millions or billions to develop are being bled out of our corporate labs ... and reentering the country **as finished products** developed by foreign entrepreneurs**."**

"The know-how of our engineering firms, **the drugs** that our pharmaceutical companies spend **billions** to develop, **the trade secrets** of our aerospace industry - these **are the bases of our national welfare."**

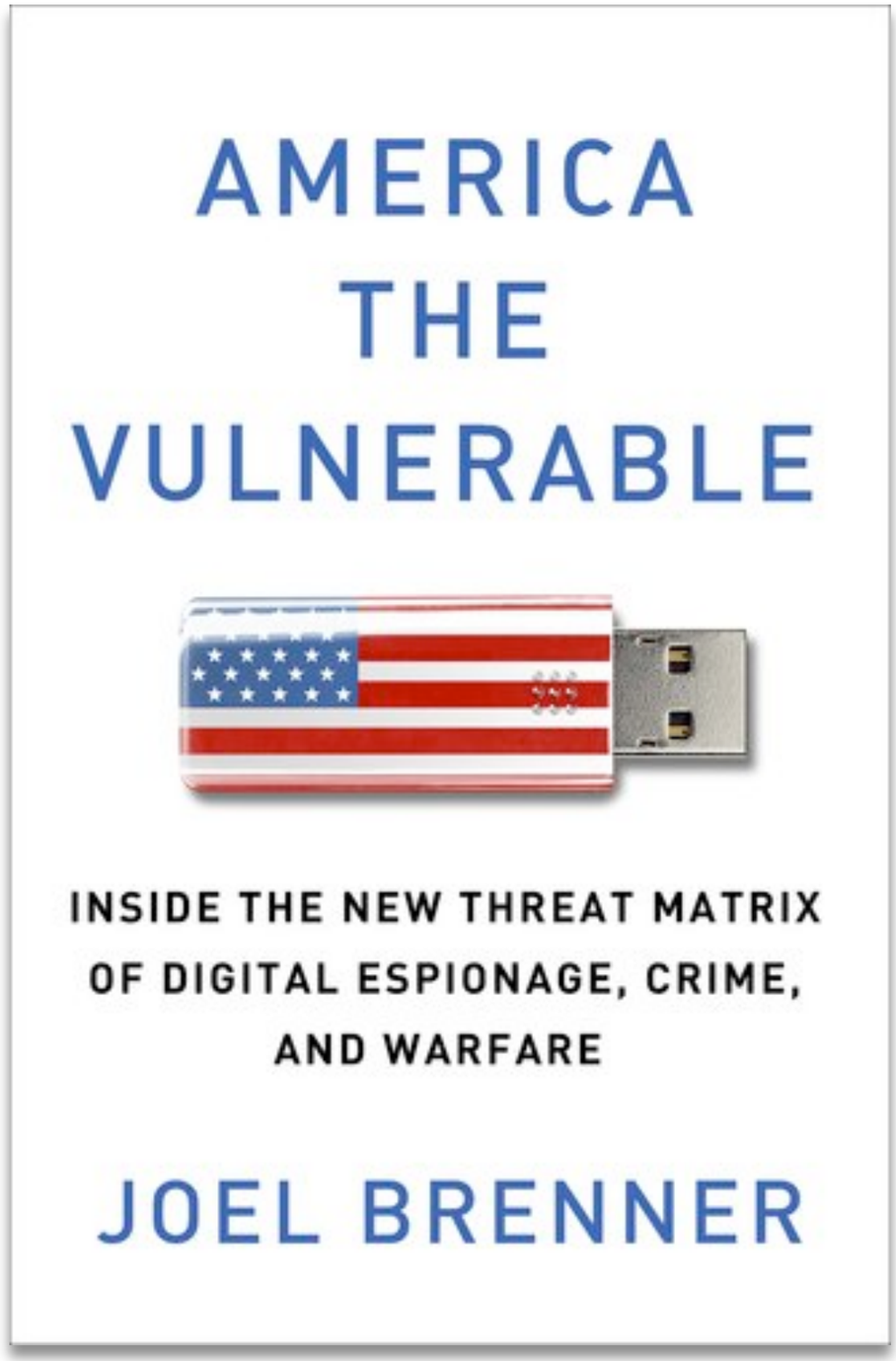


Assessment by Joel Brenner September 2011

"The boundary between national and economic security ... has eroded ... almost completely."

"When it comes to national security the boundary between public and corporate secrets has more or less vanished."

The level of public and corporate secrecy "is falling precipitously."



The challenge in the digital economy

Security & Defence Agenda
Cyber-Security 2012 Report

"The challenge in the digital economy is that no chain is stronger than the weakest link."

Christian Wernberg-Tougaard
Member of the Minister's Information Security Advisory Board at Ministry of Science, Technology and Innovation, Denmark. Member of ENISA.

Losses quoted by the UK Government

UK Government Position
Cyber Security Strategy 2011

"Recent research suggests that the **costs to the UK of cyber crime** could be in the order of **£27 billion per year** ...

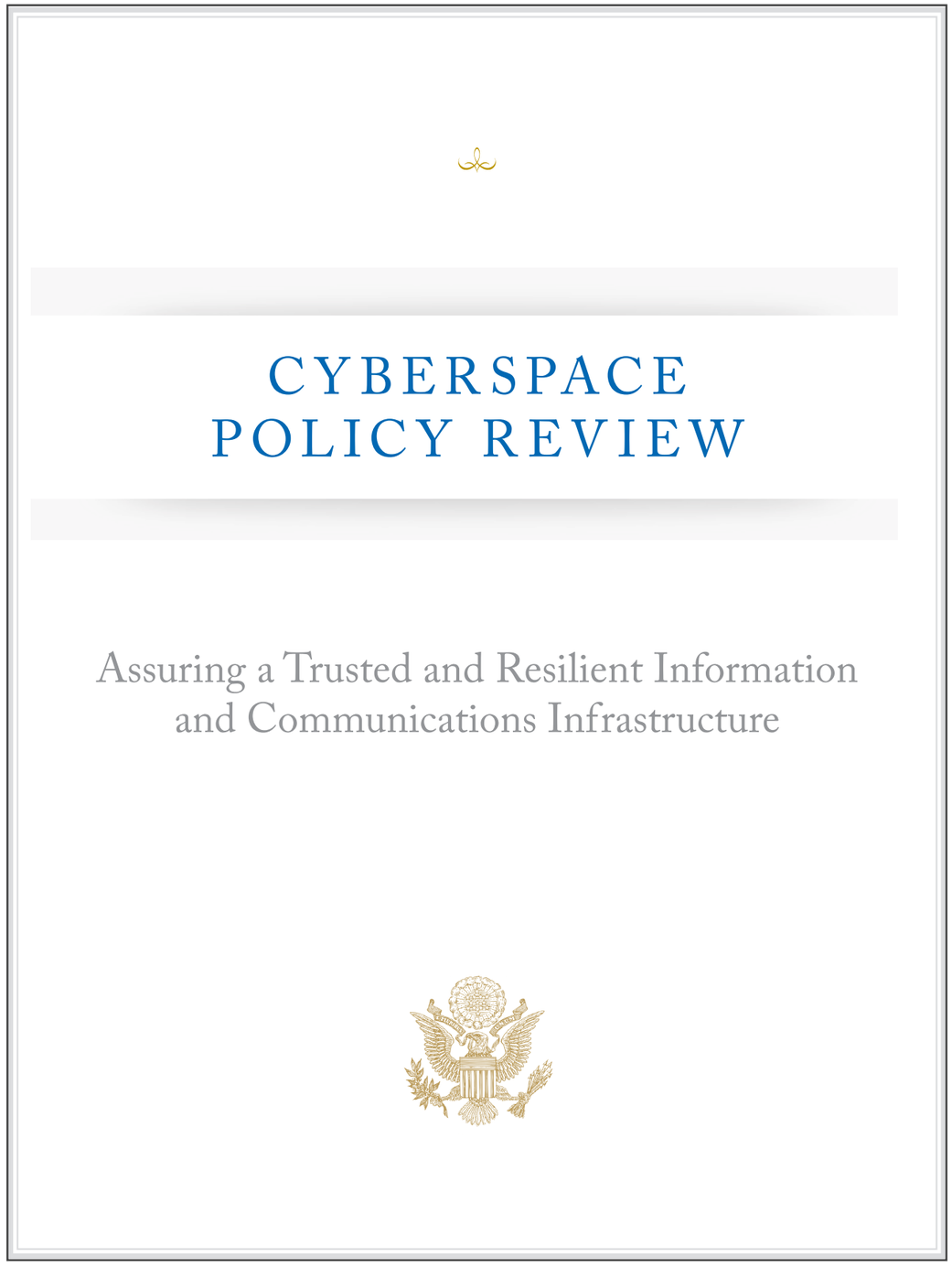
it is clear the costs are high and rising."

Losses quoted by the US Government

US Government Position
Cyberspace Policy Review

"Systemic loss of U.S. economic value:

Industry estimates of losses from intellectual property to data theft in 2008 range as high as $1 trillion."


CYBERSPACE
POLICY REVIEW

Assuring a Trusted and Resilient Information and Communications Infrastructure

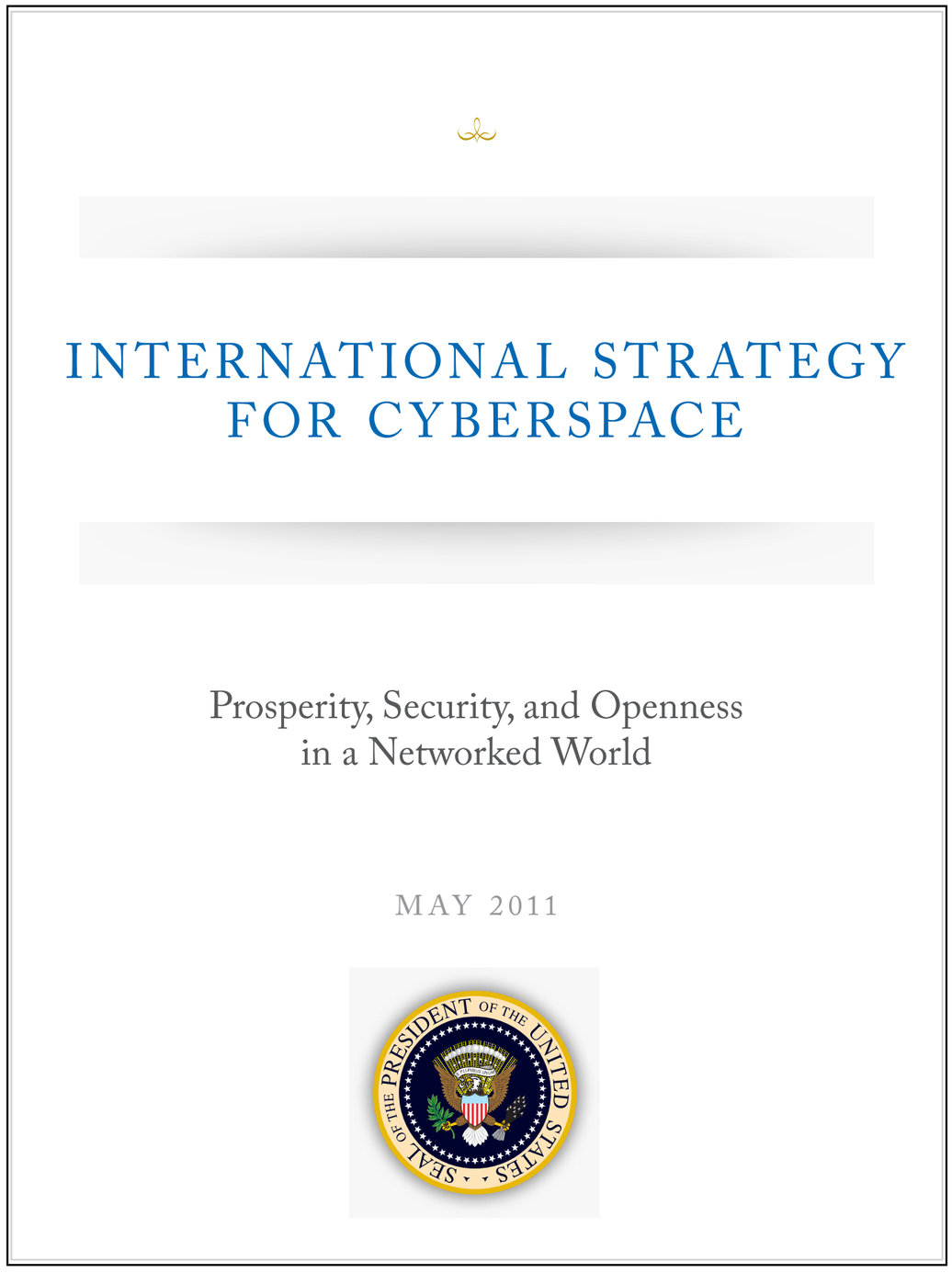
US Government advises companies of the risks

US Government Position, 2011
International Strategy for Cyberspace

"Cyberspace can be used to steal an unprecedented volume of information from businesses ...

stolen information and technology can equal billions of dollars of lost value."

"Results can range from unfair competition to the bankrupting of entire firms."


INTERNATIONAL STRATEGY FOR CYBERSPACE

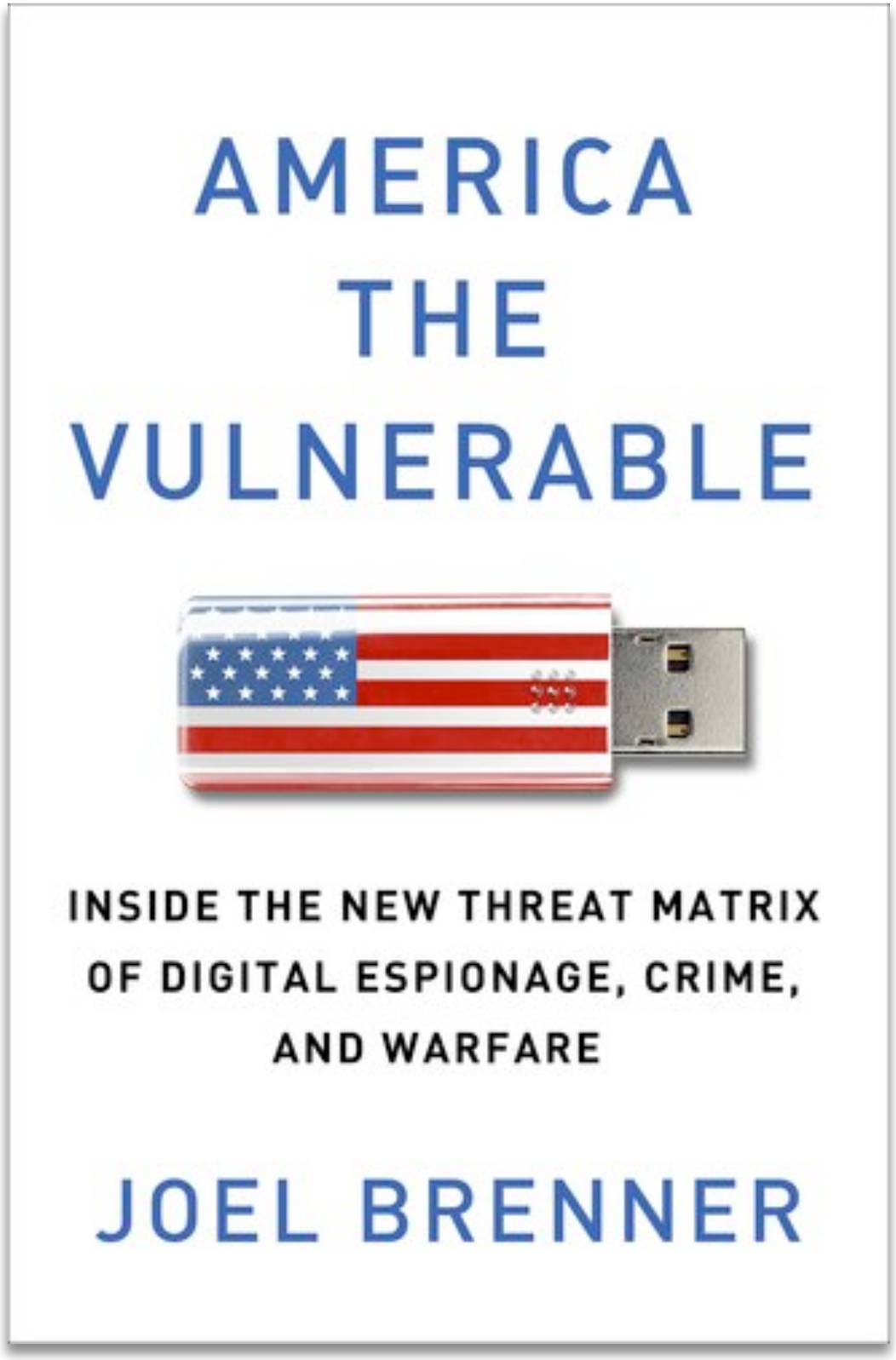
Prosperity, Security, and Openness in a Networked World

MAY 2011

Case point 1: U.S. Navy

"The U.S. Navy spent **~$5 billion** to develop a quiet electric drive for submarines and ships so they'd be silent and hard to track.

Chinese spies stole it."



Case point 2: Sony Playstation Network breach

- **Sony's PlayStation Network annual revenues $500 million**
- **The breach could cost Sony $1.5 billion, an average of $20 for each of the 77 million customers affected 2011**

– **Larry Ponemon**
Chairman and Founder
Ponemon Institute

Proven: Many successful attacks against the world's largest security companies

VeriSign®

Symantec

EMC²

DigiNotar®
A VASCO COMPANY

VASCO®
THE AUTHENTICATION COMPANY

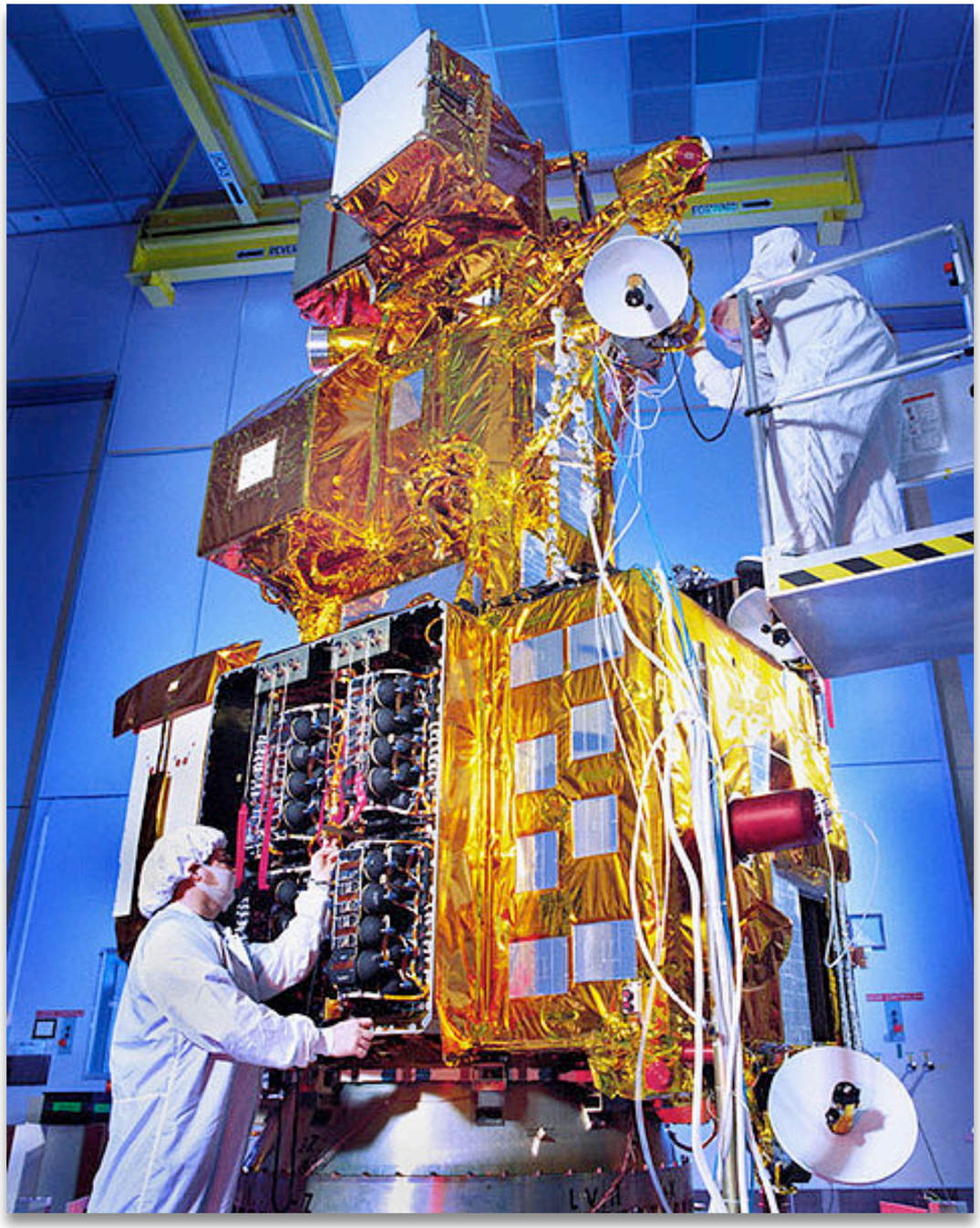
Case point 3: Bankruptcy of a Certificate Authority

VASCO®
THE AUTHENTICATION COMPANY

- DigiNotar was the Netherland Government's primary authorised PKI certificate authority
- **Owned by global security leader VASCO**
- September 2011: **Systems hacked.** Company operations taken over by Dutch Government. All Government business lost. Government, citizens and business clients exposed.
- **Company bankrupt within 3 months** and investigated by Government for possible **criminal negligence**

Case point 4: Hacked U.S. Satellites

- November 2011 USA Congressional Commission Annual Report: **Two NASA managed satellites hacked at least four times**
- The attackers had **enough access to take complete control** of one of the satellites
- Access to a satellite's controls could allow an attacker to damage or destroy the satellite
- An attacker could also deny or degrade as well as forge or otherwise manipulate the satellite's transmission

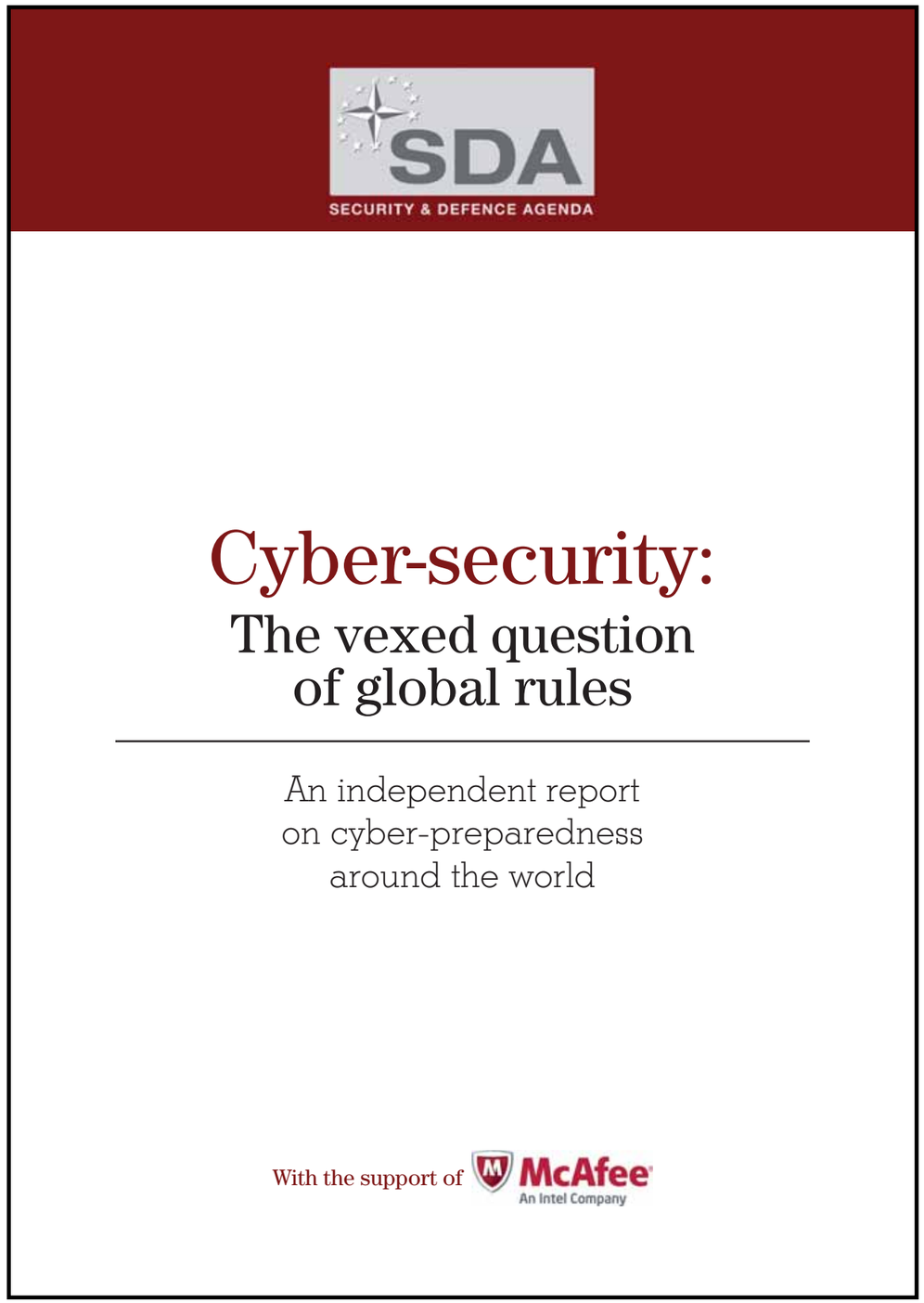


Case point 5: Stuxnet v1, v2, v3 and now Duqu

Security & Defence Agenda
Cyber-Security 2012 Report

"SCADA Systems ... are the physical elements that control pumps and barrels, and other infrastructural and industrial processes.

The challenge is that they used to be isolated systems and now they are often connected to the Internet or accessible using data transfer devices like USB sticks."



Increased connectivity means more vulnerability

Security & Defence Agenda
Cyber-Security 2012 Report

"If you can control a SCADA system, you control the facility or the industry."

- Bart Smedts

Senior Captain Bart Smedts
Research Fellow at the Belgian Royal Higher Institute for Defence. Expertise in critical infrastructure protection and cyber-defence.
Image: www.b-ccentre.be

Difficulties in protecting industrial control systems

Security & Defence Agenda
Cyber-Security 2012 Report

“Many of these systems are unprepared for cyber attacks.”

- Frank Asbeck

Frank Asbeck
Principle Counsellor for Security and Space Policy, European External Action Service

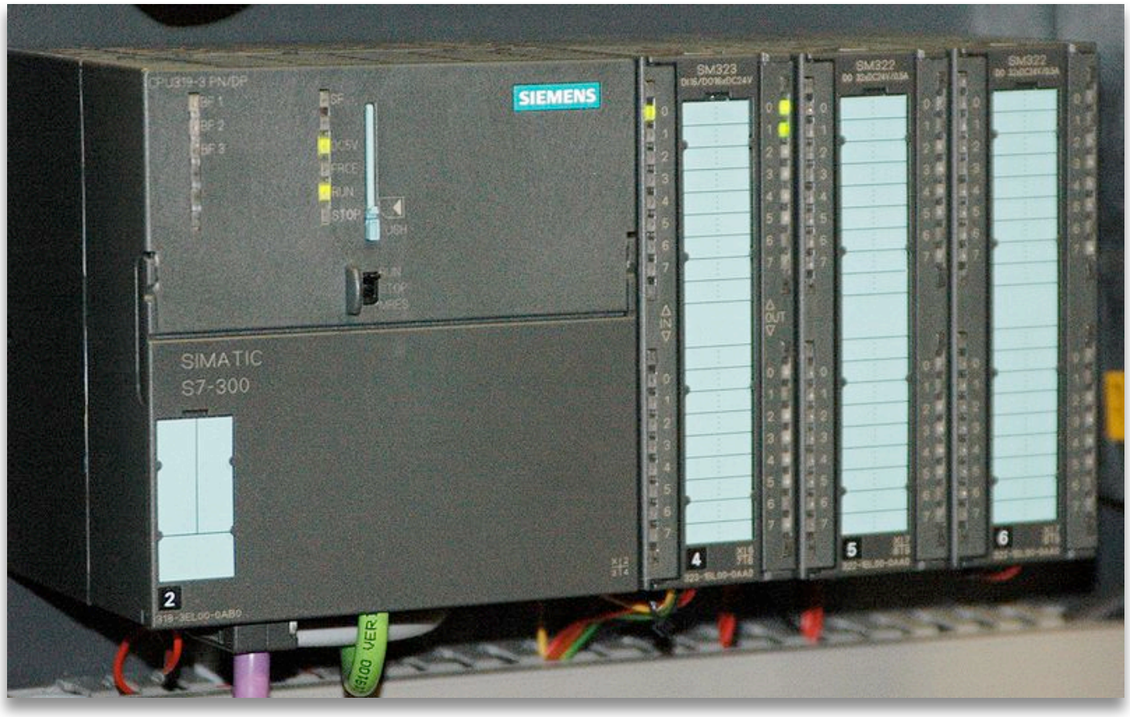
Image: © Gleamlight / Philippe Molitor

Case point 5: Stuxnet v1, v2, v3 and now Duqu

- **Critical infrastructure is proven**
  vulnerable to specialized "targeted" attacks

- **Stuxnet is a computer worm discovered in June 2010**

  - The worm spreads indiscriminately, NOW found in 155 countries
  - Spies on and subverts industrial systems
  - Spreads via Microsoft Windows, and targets Siemens industrial software and equipment
  - **Can physically damage equipment (e.g. Iran nuclear facility)**
  - New variants in 2011



Siemens Simatic PLC (Image: Wikipedia)

- **A new related spy worm discovered in September 2011 - "Duqu"**

Cyber attacks not limited to damaging centrifuges

James Andrew Lewis
Director and Senior Fellow,
Technology and Public Policy Program
U.S. Center for Strategic &
International Studies (CSIS)

In addition to the centrifuge attacks in Iran that experts say put their nuclear industry back years,

James Andrew Lewis says **actual attacks have been proven possible in the USA against other facilities/equipments**

More on this point shortly

Case point 5: Stuxnet v1, v2, v3 and now Duqu

Ralph Langner

German industrial control systems expert interview **September 2011**

- **Stuxnet code is public and being readily exploited by others**
- With Stuxnet as a “blueprint” **downloadable from the Internet**

“any dumb hacker” can now figure out how to build and sell cyberweapons

to any hacktivist or terrorist who wants “to put the lights out” in a US city or **“release a toxic gas cloud.”**

Case point 5: Stuxnet v1, v2, v3 and now Duqu

Ralph Langner

German industrial control systems expert interview **September 2011**

- “Every day cyber weapon technology proliferates
- The understanding of how Stuxnet works spreads more and more
- All the vulnerabilities exploited on the industrial control system level and programmable logic controller level are still there”

Case point 5: Stuxnet v1, v2, v3 and now Duqu

Ralph Langner

German industrial control systems expert interview **September 2011**

"Arms control with satellite surveillance is impossible.... So I'm afraid **cyber-arms control won't be possible.**

That's why the best option we have to start to counter this threat is to start protecting our systems – control systems, especially – in important facilities like power, water, and chemical facilities that process poisonous gases."

"all these control systems,
if compromised,
could lead to mass casualties,
but we still don't have any significant level of cybersecurity for them."

Case point 5: Stuxnet v1, v2, v3 and now Duqu

Dr. Sandro Gaycken argues:

- The attack on Iran was a ruse to distract from Stuxnet's real purpose
- Its broad dissemination in more than 100,000 industrial plants worldwide suggests a field test of a cyber weapon in different security cultures
- Testing their preparedness, resilience, and reactions
- All highly valuable information for a cyberwar unit

November 2010

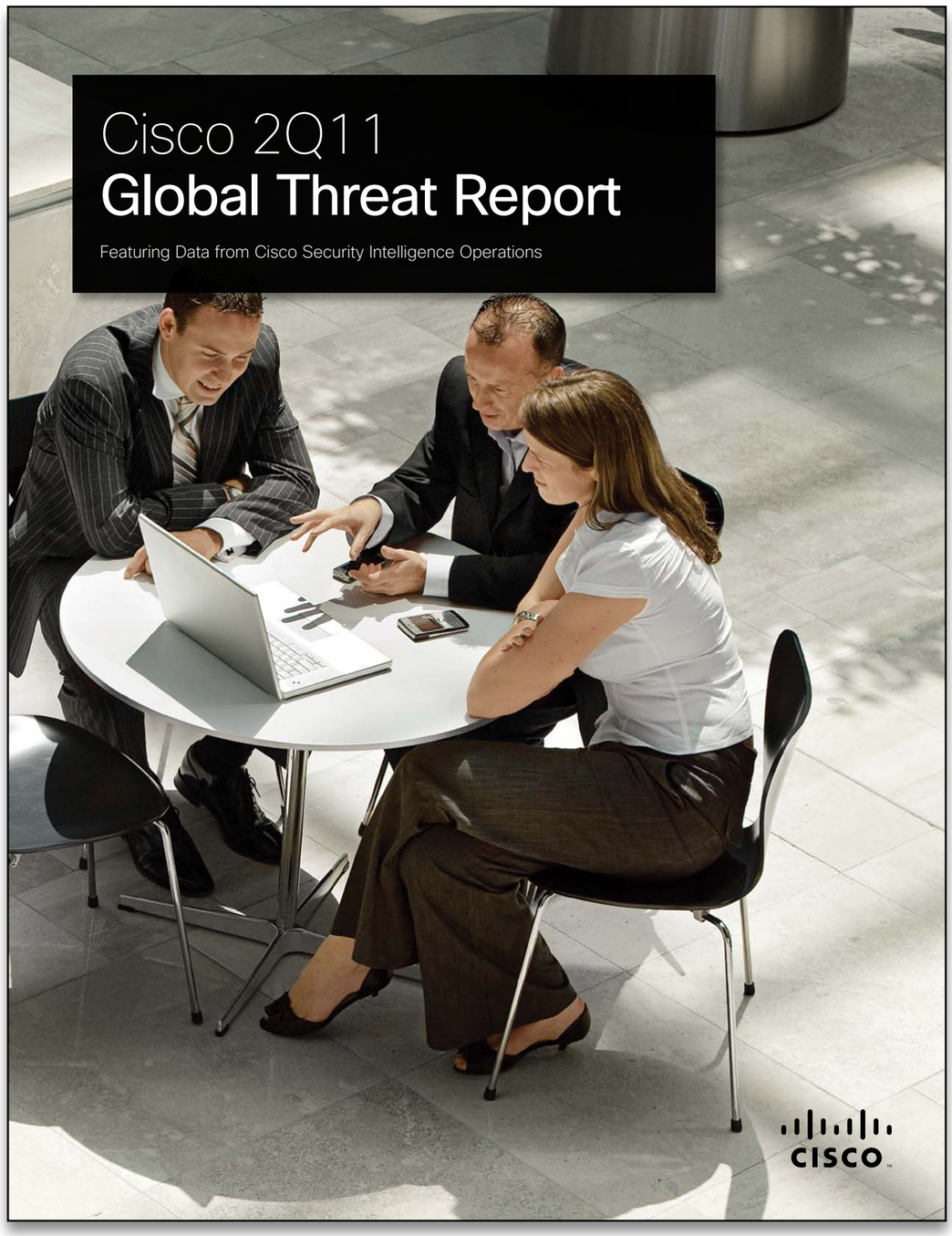
Dr. Sandro Gaycken
Free University Berlin

Image: Juliane Henrich

Case point 5: Stuxnet v1, v2, v3 and now Duqu

Cisco 2Q11
Global Threat Report

"Among the top 10 fields affected by cyber crime, **companies in the pharmaceutical and chemical industries were at the highest risk of malware attacks**"



Cyber Security for Chemical Industry Europe Conference 2012

"The words 'Nitro', 'DuQu' and 'Stuxnet' have filled board rooms **with dread and much angst** over the last few months as the trend for such cyber threats seems to be gaining momentum."

Public Proofs: Concerned experts

Ralph Langner

German industrial control systems expert interview **September 2011**

CSM: But you yourself recently decided to demonstrate how simple a Stuxnet attack could be – just four lines of code – to make an industrial system freeze. A time bomb, really. Why did you do that?

LANGNER: I couldn't stand it any longer. ... We published last September that parts of Stuxnet could be copied and that such a weapon would require zero insider knowledge. Nobody listened.
What you still hear today from all kinds of people is how a Stuxnet-type attack requires so much insider knowledge.
I finally had to publish this four-line attack just to make sure no smart-guy tells his boss that this is impossible.

Public Proofs: Wikileaks, Anonymous hackers

- **Recent increased activity demonstrate that systems of the most powerful organisations remain vulnerable today**

Case point 6: Emergency services hit 2011

- **Critical infrastructure is vulnerable to "un-targeted" indiscriminate attacks from malware that is running rampant around the Internet**

- e.g. Stuxnet. Other malware disabled the "automated response system" of St. John Ambulance service in New Zealand, 2011

  - System responsible for organising 90% of the emergency and non-emergency ambulance dispatch for New Zealand population

  - Staff were forced to allocate ambulances manually

- Medical related services of hospitals have also been impacted by common malware

Image: Wikipedia

Case point 7: Power Grid 2011

Gregory H. Friedman
INSPECTOR GENERAL
Department of Energy

Report from the US Department of Energy Inspector General
February 2011

- America's power grid remains vulnerable to cyberattack
- A result of sluggish implementation of weak computer security standards and insufficient federal oversight.

http://www.csmonitor.com/USA/2011/0203/America-s-power-grid-too-vulnerable-to-cyberattack-US-report-finds

Cyber attacks not limited to damaging centrifuges

The Atlantic and Government Executive's Cybersecurity Forum, Dec 2010

“The electrical grid.

A popular target in the military.

If you go back 30 years like in Warsaw Pact planning, one of the first things they are going to strike was the electrical grid.

Very vulnerable.

So black outs, and more importantly,
physical destruction,
which we know they can do.”

James Andrew Lewis
Director and Senior Fellow,
Technology and Public Policy Program
U.S. Center for Strategic &
International Studies (CSIS)

Video used with permission

Physical destruction of power generators

"There was, in 2007, a test at the Idaho National Labs by Michael Assante.

Michael asked: **If I was a hacker, and I hacked into the control system, kinda like stuxnet, of one of these big huge room-sized generators, what could I do to it?**

The answer is:
you can make it jump up and down, emit smoke, and shake itself to pieces.

So we know the ability to do physical destruction is there.

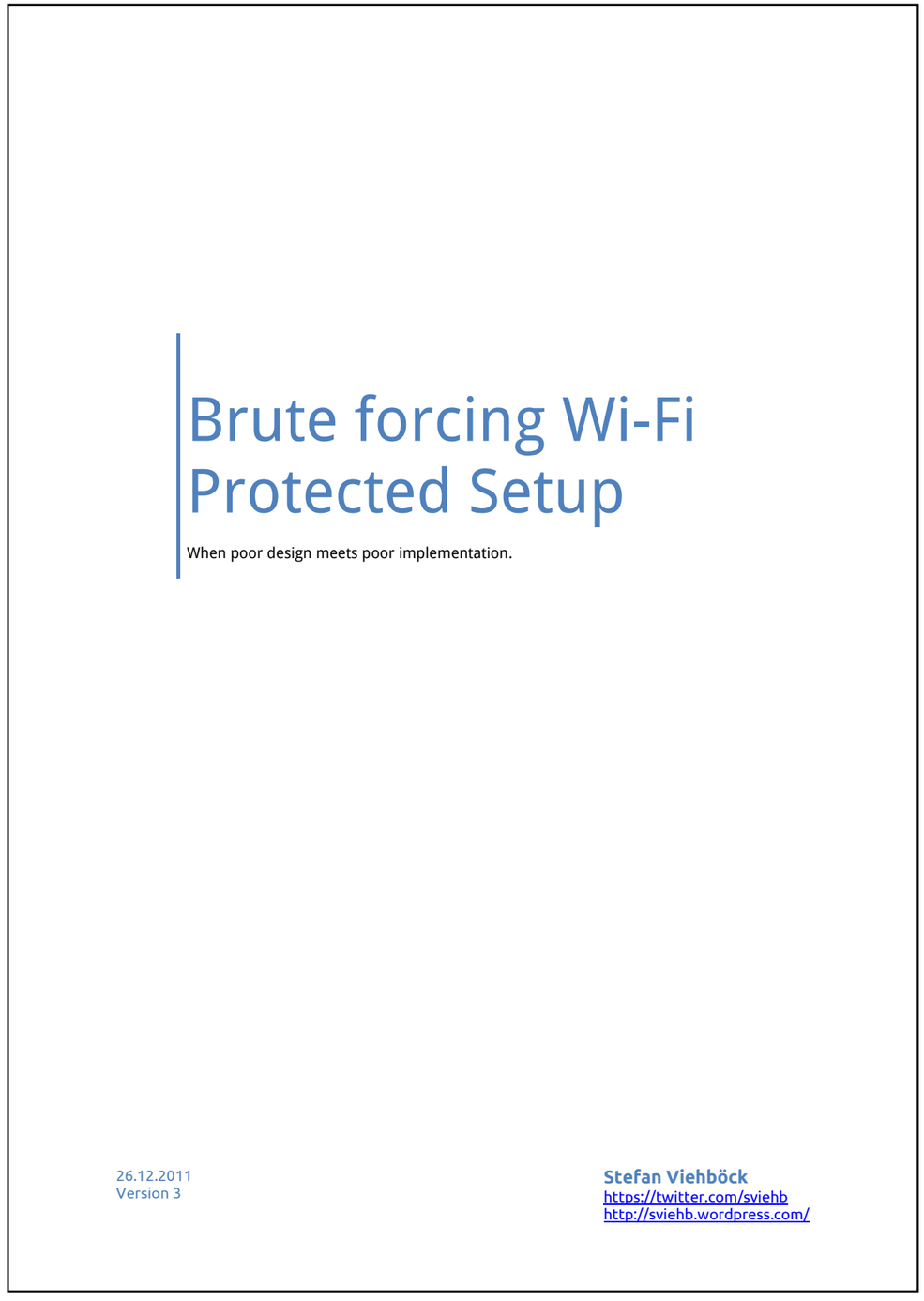
We know that from at least one episode, and maybe two."

James Andrew Lewis
Director and Senior Fellow,
Technology and Public Policy Program
U.S. Center for Strategic & International Studies (CSIS)

Video used with permission

Case point 8: Wi-Fi security failure December 2011

- Brute forcing Wi-Fi Protected Setup
  - *"**When poor design meets poor implementation**", Stefan Viehböc*
- **The industry standard** "Wi-Fi Protected Setup" (WPS) feature can be **broken** by a simple brute-force guessing attack:
  - Devices without countermeasures broken in less than 4 hours, otherwise in less than 44h
- Nearly all Wi-Fi access points are vulnerable
  - Including Cisco/Linksys, Netgear, Belkin, Buffalo, TP-Link, ZyXEL and D-Link
  - Hacker tools already exploit vulnerability
  - How many organisations at risk?



Case point 9: Unquantifiable costs to business

- **A Fortune 100 company experience:** 2009 - 2010
  - A victim of the zero-day PDF attacks sent via emails
  - 400% increase in intrusions over two weeks
  - **"That attack resulted in unquantified losses for that company.**

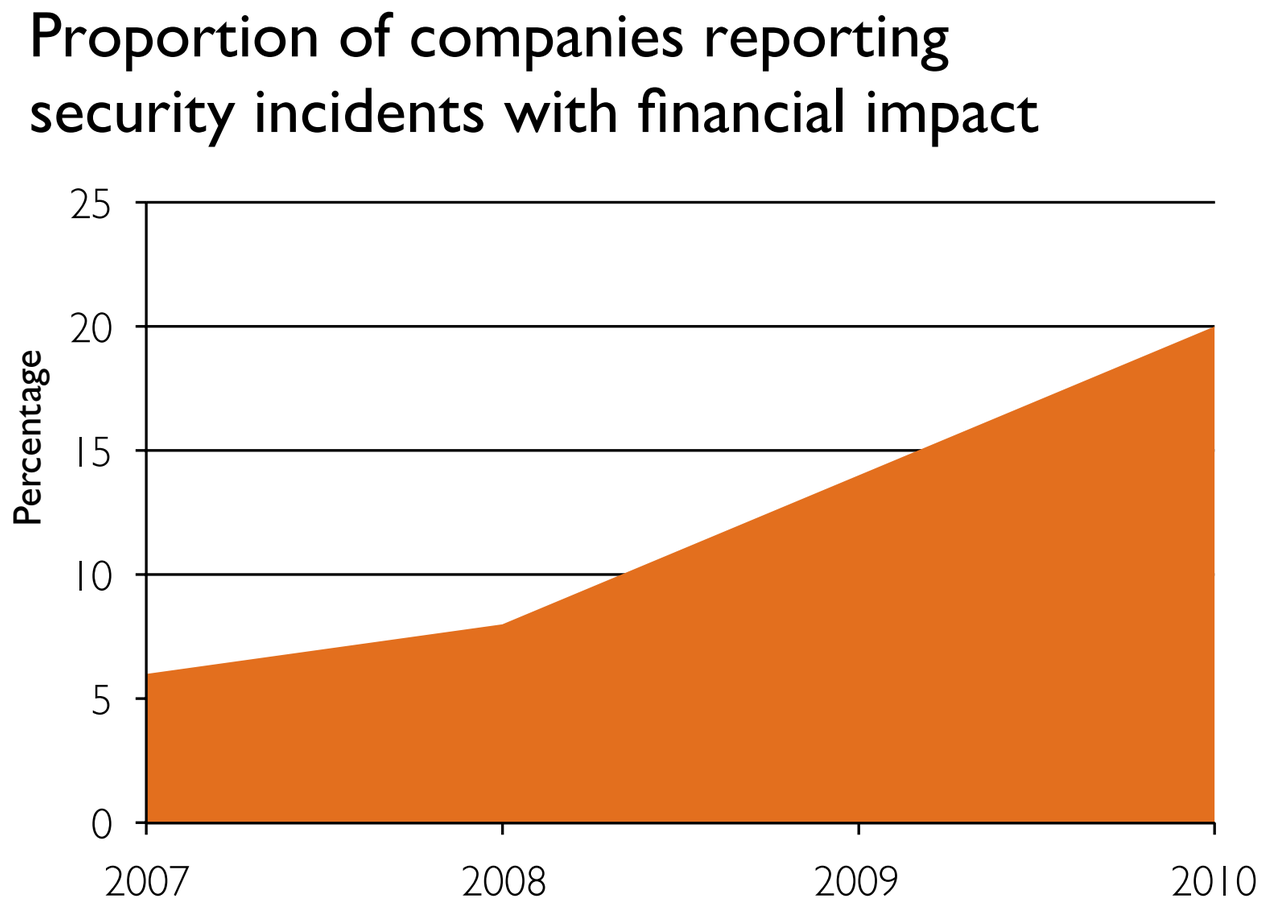
    Think about **how many man hours** a fortune 100 company needs **to test all of those networks** to see how many intrusions, hundred and thousands, **millions of intrusions**,

    how many actually made it **into the core infrastructure?"**

Melissa Hathaway
Led U.S. President Obama's Cyberspace Policy Review

(video used with permission)

How **LOW** are **your** cyber security defences?



Source: *Pricewaterhouse Coopers. Global state of information security survey, 2011*

"If citizens feel threatened, mistrustful and increasingly hesitant towards innovative applications and services, our whole society may end up being the loser."

– EU FP7 RISEPTIS Report 2011

What level of assurance do we have in today's Information and Communication Technologies?

"Today's Trust Bubble products are rife with a huge pile of crippling un-addressed conceptual and implementation debt."

Brian Snow
November 2011

Synaptic Labs' Annual Report on the Global Cyber Security Status 2012

1. High level overview
2. Global assessments and global responses
3. The stability of Nations is at risk
4. Our cyber defences are very low
5. **Experts: The cyber risk is not overstated**
6. Closing statement
7. Related videos

The Atlantic and Government Executive's Cybersecurity Forum, Dec 2010

Videos online: http://events.theatlantic.com/cyber-security/2010/

The Atlantic and Government Executive's Cybersecurity Forum, Dec 2010

"Whatever happens with IT, cyber security will be pulled right there, because again it becomes the enabler.

So this is big business,

and we are just now recognising it to the point where we are putting major resources against it."

Vice Admiral J. Mike McConnell (USN Ret)
Intelligence Adviser to President Obama 2009

The Atlantic and Government Executive's Cybersecurity Forum, Dec 2010

Question:

"Is there any chance, that because it [ed: cyber security] **is big business, that there is overstatement of the threat?"**

(Video footage used with permission)

The Atlantic and Government Executive's Cybersecurity Forum, Dec 2010

"I would assert that having had a privileged position as a director of NSA when we moved from cold war to current circumstances (where we went from a wireless world to a wired world) and then the business engagement I had, and also the seat I was privileged to occupy as the Director of National Intelligence,

I became convinced in the early 90's that this is a major major strategic consideration for the country.

And it is only being reinforced at an accelerating rate ever since then."

Vice Admiral J. Mike McConnell (USN Ret)
Intelligence Adviser to President Obama 2009

The Atlantic and Government Executive's Cybersecurity Forum, Dec 2010

“This is a great forum, we wouldn't have had this forum just a few years ago.

People are actually interested in this.

The University of Maryland just opened up a cyber security centre last week (December 2010), **so people are recognising it for the level of significance that it is.”**

Vice Admiral J. Mike McConnell (USN Ret)
Intelligence Adviser to President Obama 2009

The Atlantic and Government Executive's Cybersecurity Forum, Dec 2010

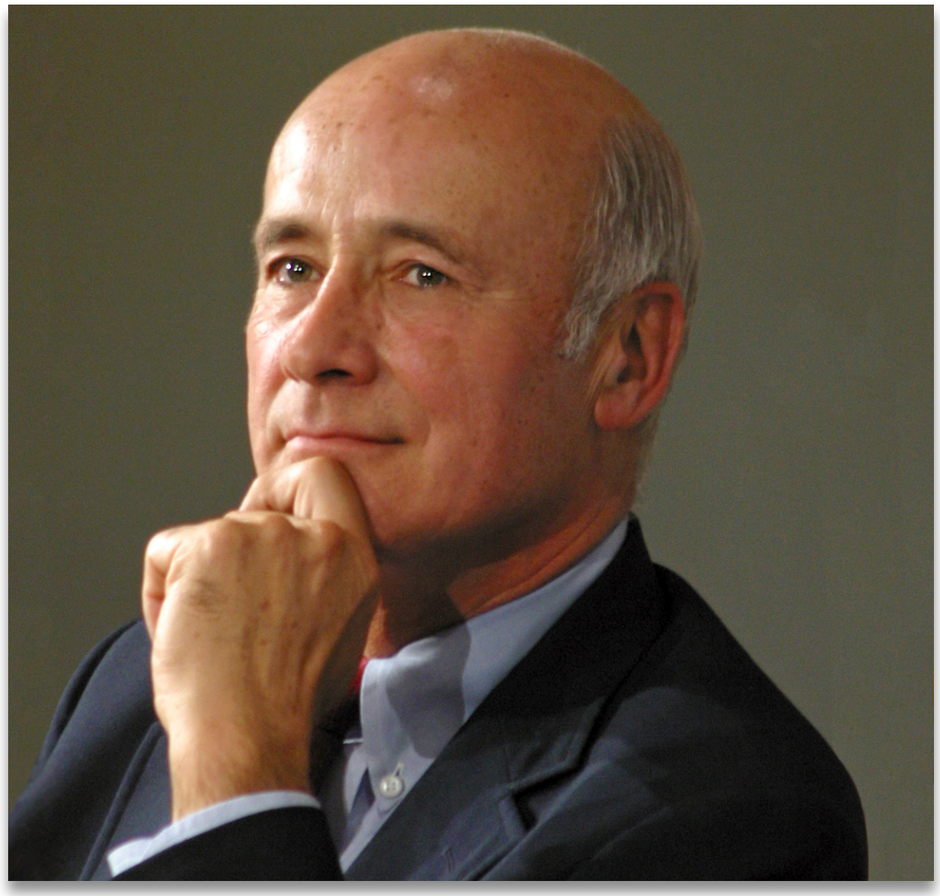
Question: “Joe do you want to grapple with the level of the threat, and what we are really talking about?”

Joe:

“We started a cyber discussion group at Harvard about 2 years ago (2008), and **the first premiss was that this threat had been hyped.** We started with the null hypothesis.

The more we learned,
The more we realised it wasn't.

I think Mike is right.”



Joseph S. Nye, Jr
University Distinguished Service Professor, the Sultan of Oman Professor of International Relations and former Dean of the Kennedy School

The Atlantic and Government Executive's Cybersecurity Forum, Dec 2010

“Going back to the business question..

One of the things to bear in mind, people always say that technology changes too fast.

And that is not true.

But there are periodic changes, maybe every decade or so, and we are changing how we connect to the Internet, that is going to affect business models.

So a lot of the companies that make stuff now, will find their business models being eroded.”

James Andrew Lewis
Director and Senior Fellow, Technology and Public Policy Program
U.S. Center for Strategic & International Studies (CSIS)

The Atlantic and Government Executive's Cybersecurity Forum, Dec 2010

"We will have a different kind of security, probably the same kind of threat, and a different kind of technology.

So when you do your analysis of how big is the market?

Remember the market leaders today will not be the market leaders 5 years from now."

James Andrew Lewis
Director and Senior Fellow, Technology and Public Policy Program
U.S. Center for Strategic & International Studies (CSIS)

The Atlantic and Government Executive's Cybersecurity Forum, Dec 2010

"**We briefed Dr Kissinger** several years ago **on the threat** and the issues and so on.

For those of you who had the pleasure of briefing Dr. Kissinger, if it's a long briefing, there are periods of time where you not sure if he is actually awake or listening.

So, this was a long discussion, and I wasn't sure, and he was asking a question occasionally. Towards the end of it, he perked up and I was waiting now for wisdom, and he said:

"Gutenberg"

Vice Admiral J. Mike McConnell (USN Ret)
Intelligence Adviser to President Obama 2009

The Atlantic and Government Executive's Cybersecurity Forum, Dec 2010

"And we just waited for the next part and he said Gutenburg.

I said Dr. Kissinger, help us.

Gutenburg invented the printing press, and it took 300 years to change the world.

You are describing a technology that has changed the world in less than a generation and our Governmental institutions **have not kept pace to understand it, or to deal with it."**

Vice Admiral J. Mike McConnell (USN Ret)
Intelligence Adviser to President Obama 2009

The Atlantic and Government Executive's Cybersecurity Forum, Dec 2010

"I thought that was an incredible way to talk about this issue. It's moving so fast, and it touches us all in so many different ways.

The one that I usually go to is banking.

The world cannot function without an effective banking system, and it is possible to contaminate the database upon which banking operates.

There is no gold standard, no dollar bills, so if you can just contaminate the data in one large bank, you could cause global banking to collapse."

Vice Admiral J. Mike McConnell (USN Ret)
Intelligence Adviser to President Obama 2009

The Atlantic and Government Executive's Cybersecurity Forum, Dec 2010

"I would just say,

I don't believe at all that we are overstating the threat.

There isn't a day that goes by that I don't hear about some attempt, some threat, some vulnerability, against the domain that I'm responsible for.

Quite frankly, open press on a daily basis we are now hearing about it.

I think we are not at all overstating the threat."

Debora Plunkett
Director of the Information Assurance Directorate (IAD)
U.S. National Security Agency

The Atlantic and Government Executive's Cybersecurity Forum, Dec 2010

"We have the capacity of certainly the U.S. Government, many industry partners, and academia.

We really need to be galvanising our resources,

to develop and deliver innovation in ways that we might better protect and defend."

Debora Plunkett
Director of the Information Assurance Directorate (IAD)
U.S. National Security Agency

Synaptic Labs' Annual Report on the Global Cyber Security Status 2012

1. High level overview
2. Global assessments and global responses
3. The stability of Nations is at risk
4. Our cyber defences are very low
5. Experts: The cyber risk is not overstated
6. **Closing statement**
7. Related videos

Global risk, global responsibility, united in action

- Being interconnected and interdependent means
  cyber security is a shared responsibility
  at home and in the global village

- Most nations have joined international cyber security efforts

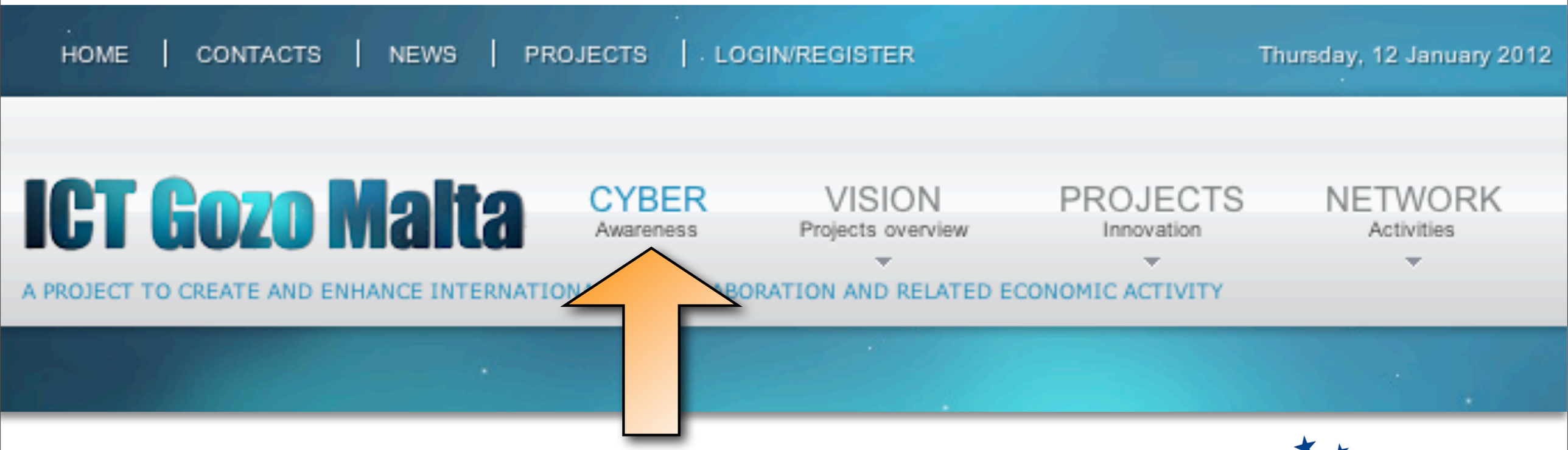
- Many have launched national cyber awareness campaigns
  to engage the public

IMPACT
INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

COMNET
Foundation for ICT Development

Get fast access to many cyber security resources

www.ictgozomalta.eu



GET SAFE ONLINE .org TM

be SMART ONLINE!

ins@fe

enisa European Network and Information Security Agency

STAY SMART ONLINE

The global community should get involved...

Vice Admiral J. Mike McConnell (USN Ret)
Intelligence Adviser to President Obama 2009

"the U.S. Cybersecurity Initiative is primarily to protect **.mil** and **.gov** information

Somebody should worry about .com

98% of the world is **.com** or **.edu** or **.org** or a foreign segment of the global Internet"

Addressing core problems for the 100%

- The ICT Gozo Malta Project is addressing core problems to protect the legitimate interests of all sectors of the global community
  - From personal through business all the way to critical infrastructure protection

Synaptic Labs' Annual Report on the Global Cyber Security Status 2012

1. High level overview
2. Global assessments and global responses
3. The stability of Nations is at risk
4. Our cyber defences are very low
5. Experts: The cyber risk is not overstated
6. Closing statement
7. **Related videos**

Related videos

- Introduction to Synaptic Labs 2012
- Synaptic Laboratories Ltd's Annual Reports 2012:
  - On the Cyber Security Problems, Drivers and Incentives
  - On the Vision, Technologies, Product Development and Go-to-Market Strategies
- Brian Snow, *"Our Security Status is Grim and the way ahead will be hard"*, Malta International Cyber Awareness Seminar, Nov 2011

http://synaptic-labs.com/resources/streaming-videos

Contact: **Benjamin GITTINS**

Chief Technical Officer
Synaptic Laboratories Limited

Email: cto@pqs.io

Phone: +356 9944 9390

Web: http://synaptic-labs.com