SYNAPTIC LABORATORIES LTD.

ICT Gozo Malta

# Today's Global Cyber Security Status *and* Trustworthy Systems That Leverage Distrust Amongst Sovereigns

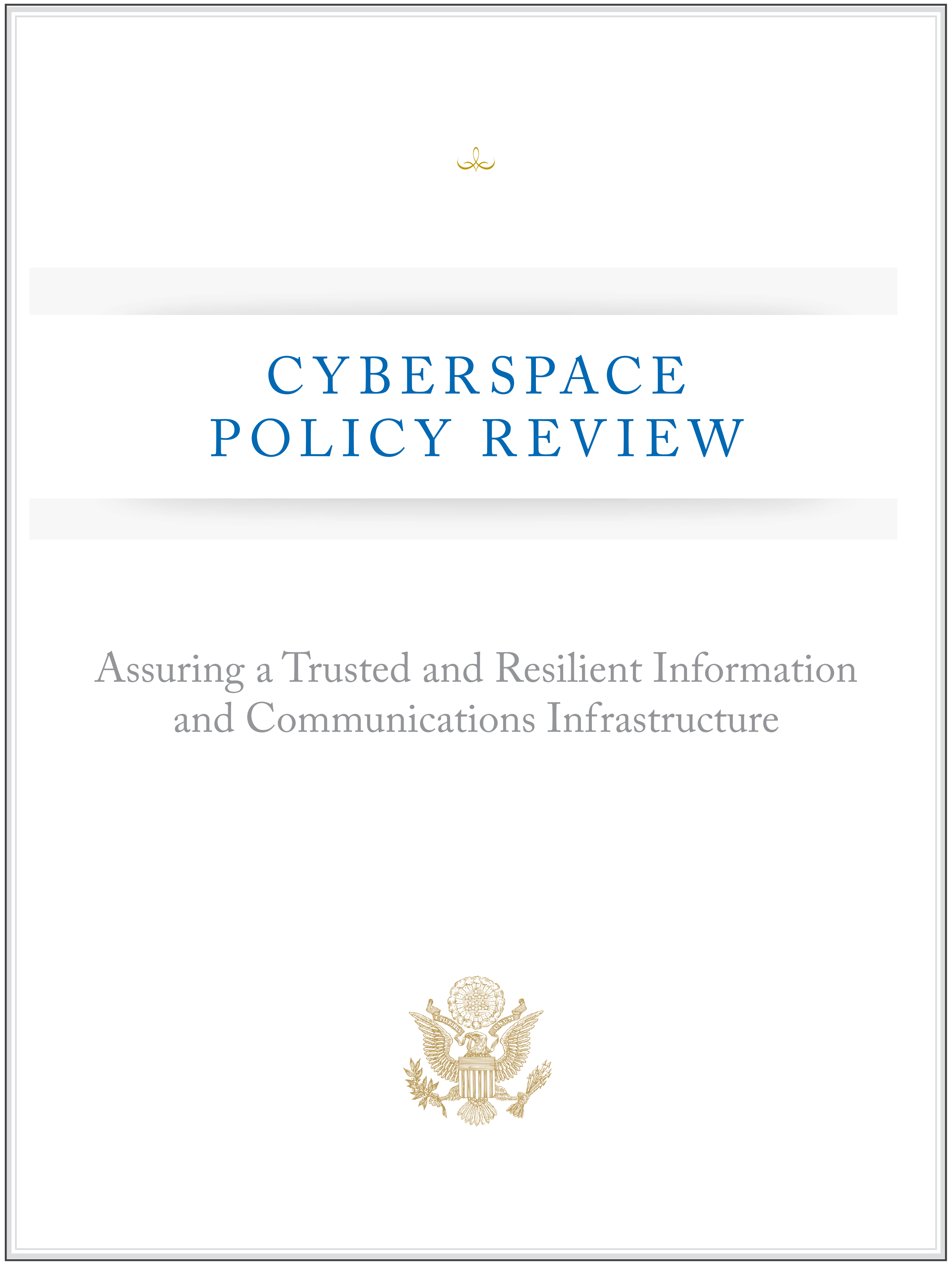
Benjamin GITTINS

Ronald KELSON

# What is cyberspace and why is it so important?

**US Government**
*Cyberspace Policy Review*

**“cyberspace .. underpins almost every facet of modern society** and provides **critical** support for the U.S. economy, civil infrastructure, public safety and national security.”



CYBERSPACE
POLICY REVIEW

Assuring a Trusted and Resilient Information
and Communications Infrastructure

# SERIOUS cyber dependency problems

**UK Government**
*Cyber Security Strategy 2011*

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

...

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

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

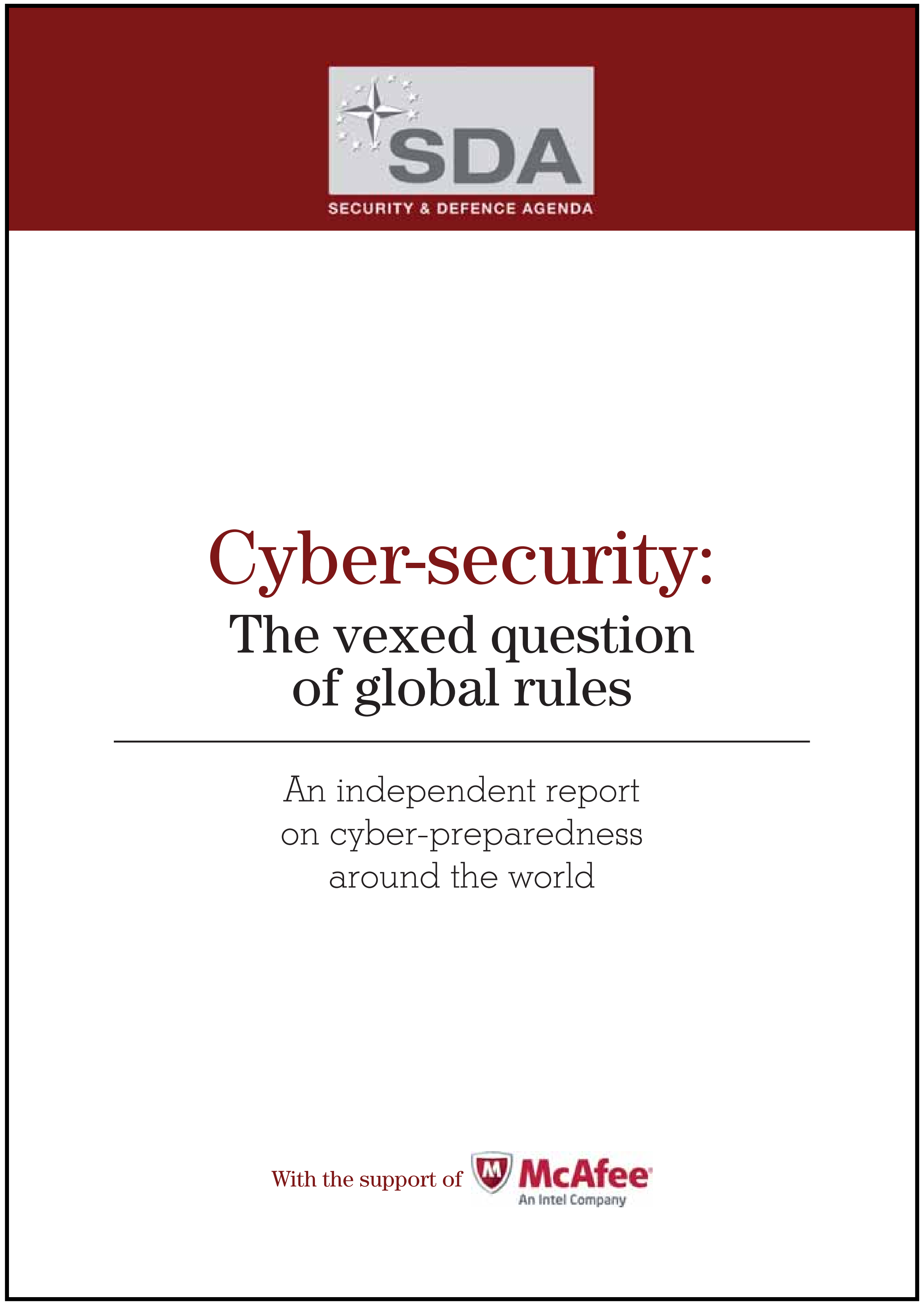
November 2011

# Global Perspectives on the Cyber Risk

**Security & Defence Agenda**
*Cyber-Security 2012 Report*

**Survey of 250 world leaders in 35 countries:**

- **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**
- **57% believe a cyber arms race is taking place**



SDA
SECURITY & DEFENCE AGENDA

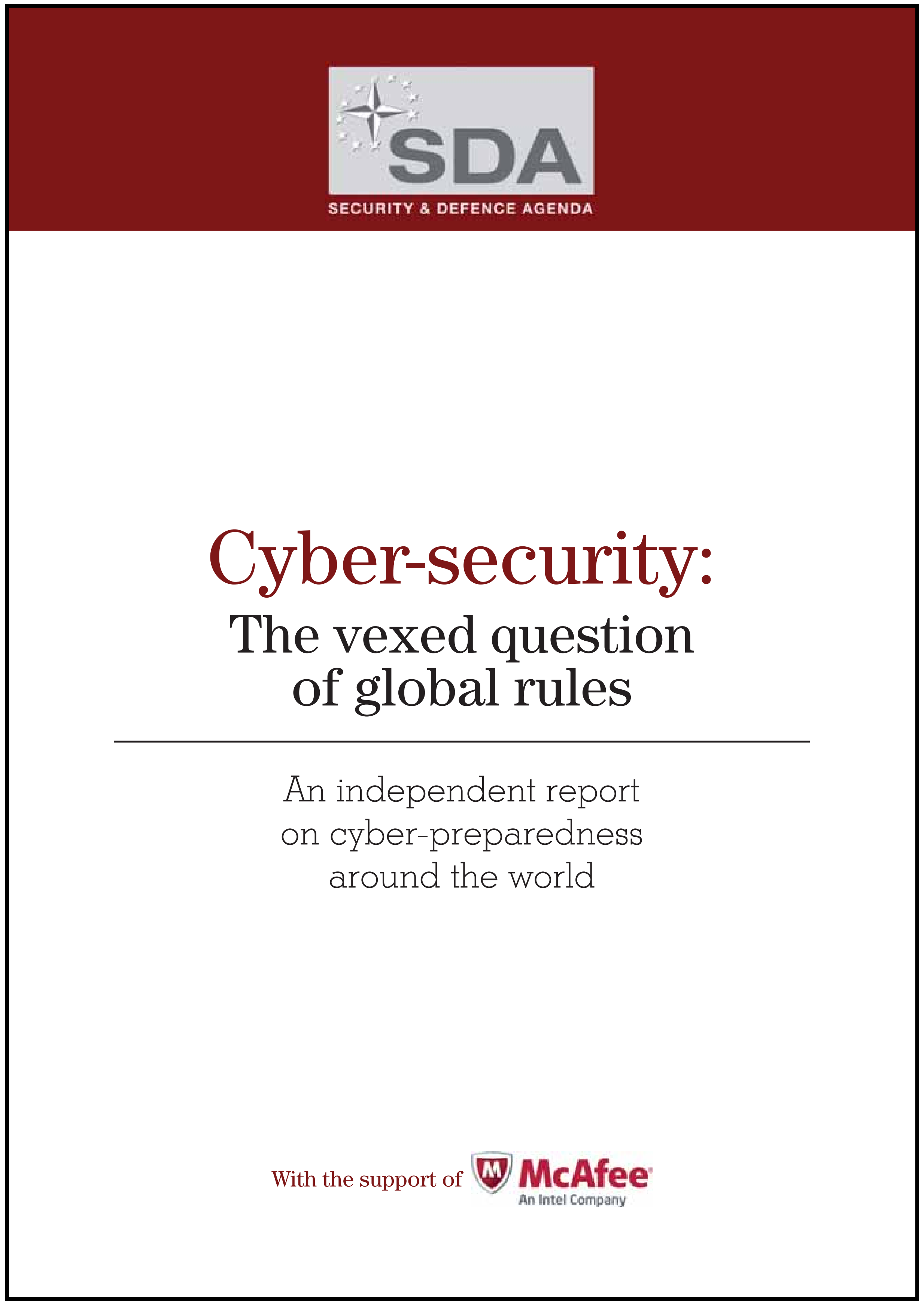
Cyber-security:
The vexed question
of global rules

An independent report
on cyber-preparedness
around the world

With the support of McAfee
An Intel Company

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

“a national threat with **wide economic consequences**.”



SDA
SECURITY & DEFENCE AGENDA

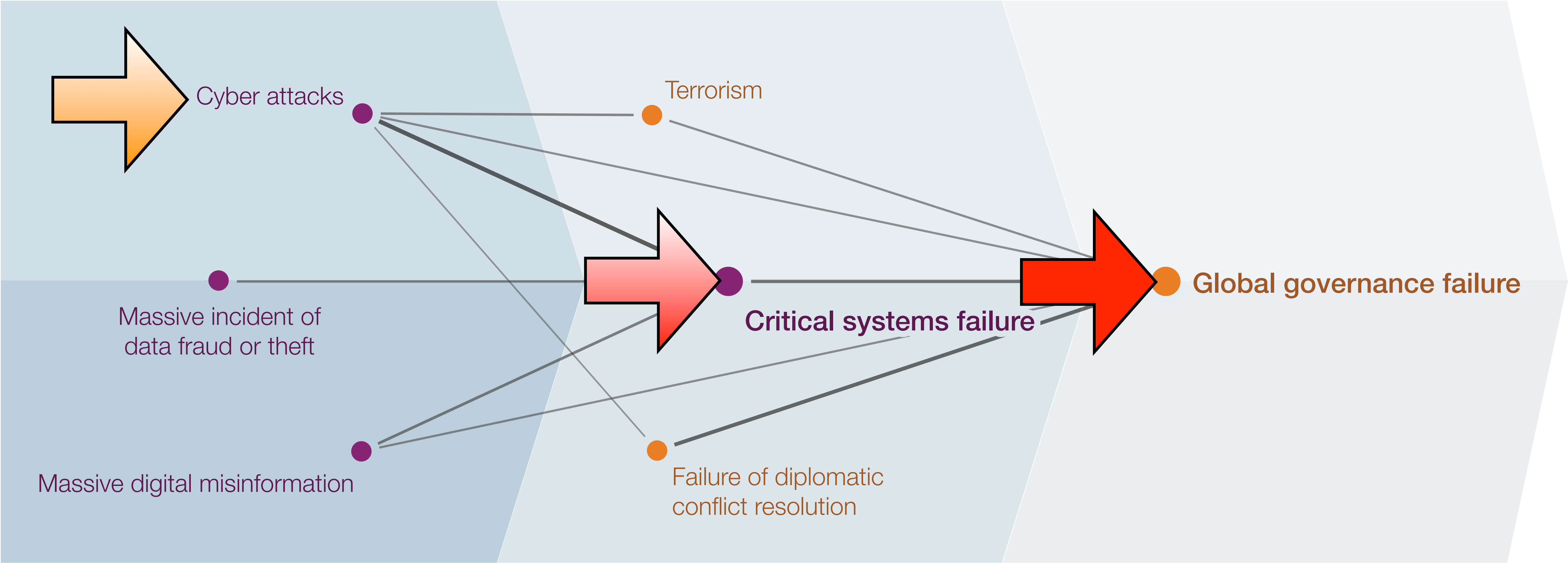
Cyber-security:
The vexed question of global rules

An independent report
on cyber-preparedness
around the world

With the support of McAfee
An Intel Company

# Most likely cause of global governance failure? Critical systems failure due to cyber attacks

**World Economic Forum**
*Global Risks 2012 Report*


Cyber attacks
Terrorism
Massive incident of data fraud or theft
Critical systems failure
Global governance failure
Massive digital misinformation
Failure of diplomatic conflict resolution

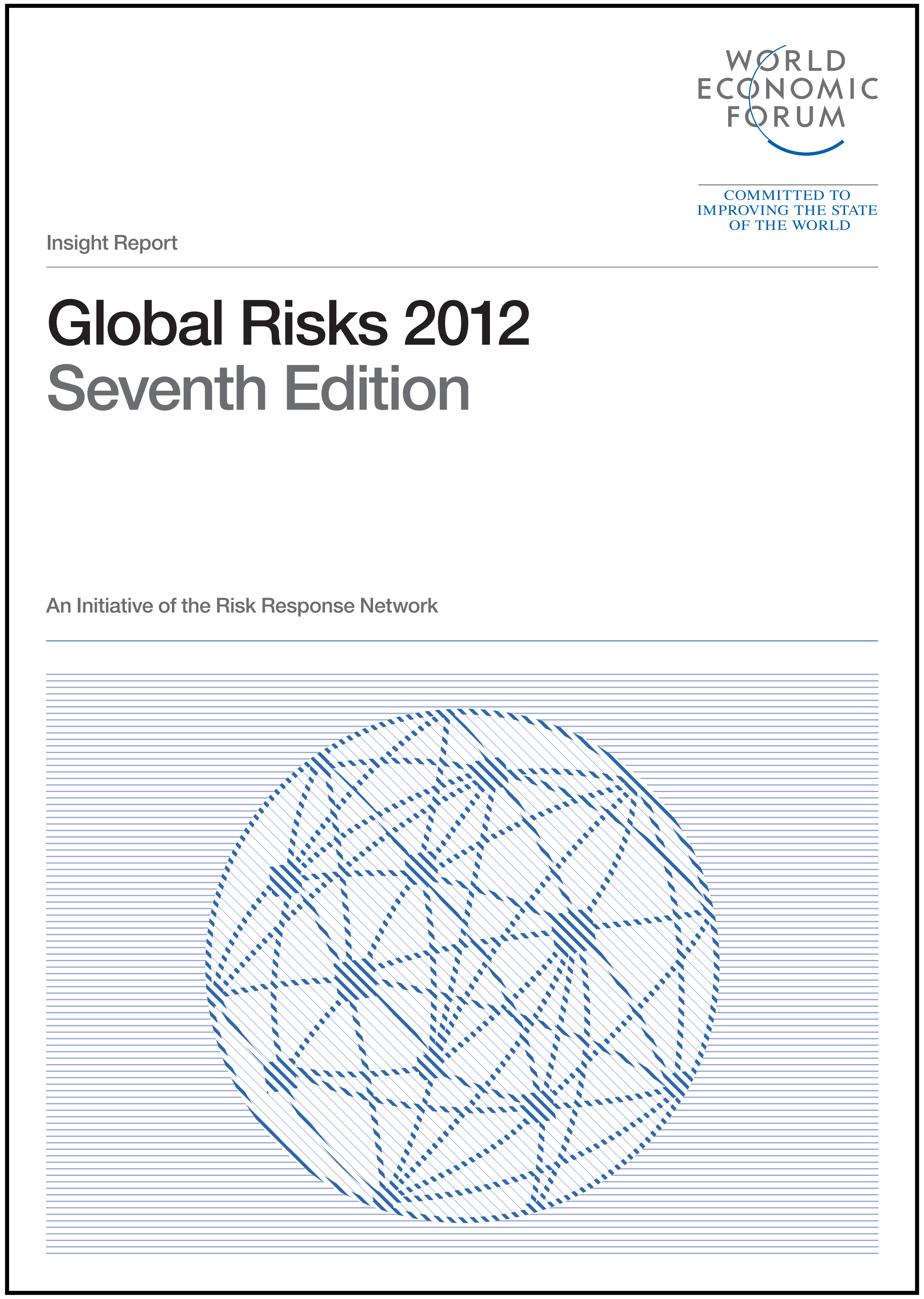
# Critical systems failure

- Occurs when a single failure triggers cascading failures in the critical infrastructure and networks
  ( *ed*: *escalating the risks of nuclear mishap, mistake and war* )

- Identified as "a key concern for world leaders from government, business and civil society."

- "most likely be caused by cyber attacks"

- Cyber attacks rank
  4th out of 50 global risks



WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Insight Report

Global Risks 2012
Seventh Edition

An Initiative of the Risk Response Network

# Cyber attacks to divert existential threats?

"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's
Ministry of Defense
(1998-)

# Case point:  Stuxnet computer Worm

- **Critical infrastructure is proven vulnerable**
- **Stuxnet:**
  - **Spreads indiscriminately** - NOW found in **155** countries
  - Spies on and subverts industrial systems
  - **Can physically damage equipment** e.g. Iran nuclear facility (*NB: different cyber attacks have destroyed room sized generators*)
- Found in more than **100,000 industrial plants worldwide** - suggests a **field test** of a cyber weapon in different security cultures

Siemens Simatic PLC

# Another big problem: cyber attack attribution

“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’.** ”

You cannot **physically threaten** or **retaliate** against a person or state you cannot **identify** or hold liable - enabling third parties to escalate confrontations!

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

November 2011

# To summarise

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

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

– **Debora Plunkett (2011)**
Director
Information Assurance Directorate (IAD)
U.S. National Security Agency

# Introducing Brian Snow

Brian Snow

**35 years in the USA NSA**

- **12 years as Technical Director**
- **Many** U.S. government and military **systems deploy his algorithms**;

  including **nuclear command and control**

# The stability of nations is at risk

Brian Snow

"I am here to tell you
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

# Fear of national strategic failure fuels cyber arms race — approx. 140 countries

- **e.g. DARPA’s global-scale cyber offensive initiative “Plan X” will *“support development of fundamental strategies and tactics needed to dominate the cyber battlespace.”***
- An effective cyber offense capability ***requires*** exploitable vulnerabilities in all potential target systems; **it requires collective ICT weakness.**

# Our four key strategies for managing the risks

**“We can't** misplace our **trust**
in different components of the system
that might have **already been violated**.

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

**Debora Plunkett**

## Strategy 1.
## Design ICT for human trust

# Our four key strategies for managing the risks

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

**Debora Plunkett**

## Strategy 2.
## Design ICT to be dependable during insider and outsider attacks,

including:

- **management or technical personnel attacks;** *and*
- **covert malware in the hardware and software (introduced during manufacture or later)**

ICT systems are NOT designed to safety standards that match our level of dependence on them

Strategy 3.
Holistically converge Safety and Security capabilities into ICT
so modern global society can Trust and Depend on ICT

# Strategy 4. Resolve architectural flaws in the design of computers

**Brian Snow**

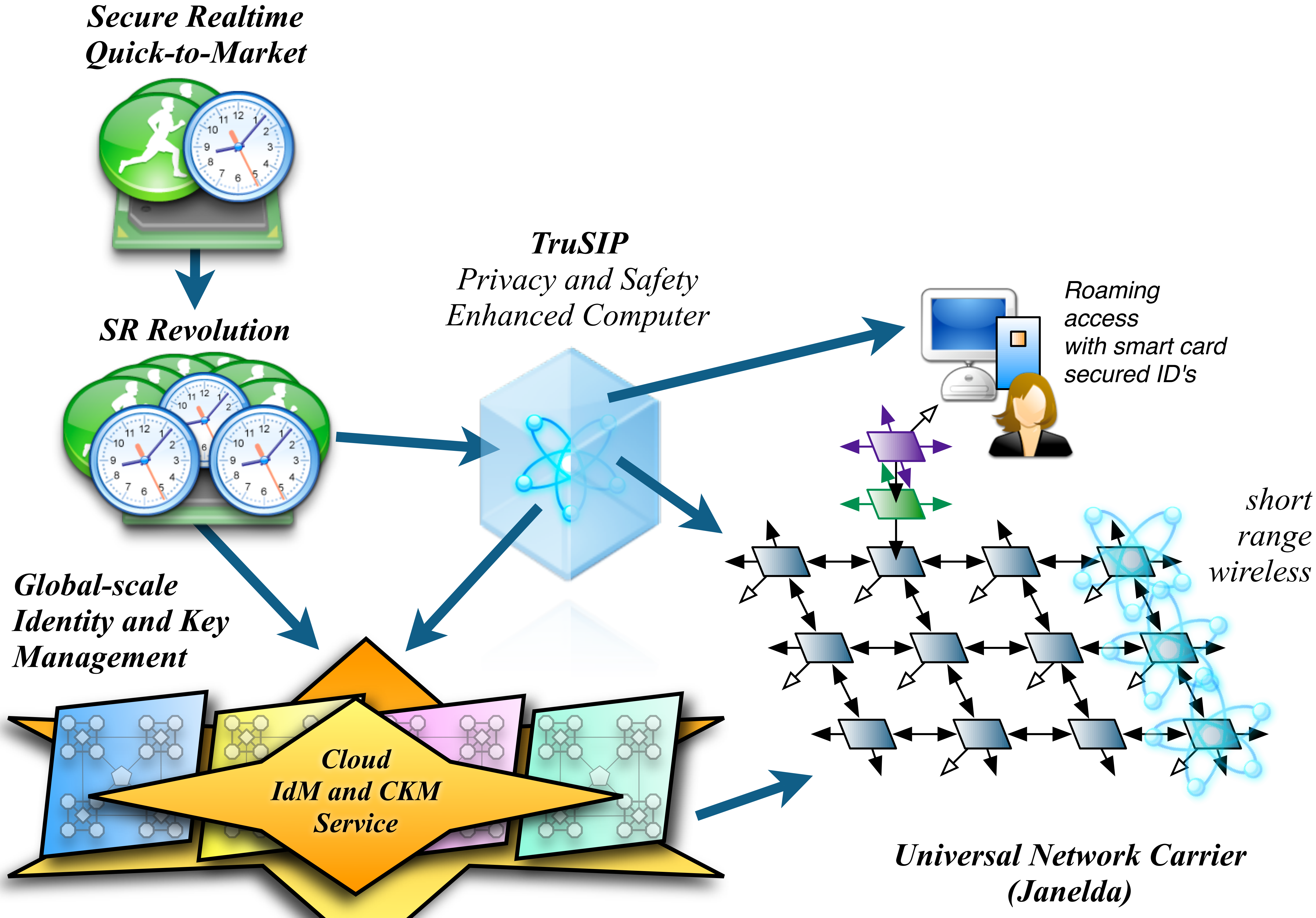
**“If you look for a one-word synopsis of computer design philosophy**,
it was ***and is:*** **SHARING**.

**In the security realm,** the one word synopsis is **SEPARATION**: keeping the bad guys away from the good guys’ stuff!

So today, **making a computer secure requires** imposing a “**separation paradigm**” **on top of** an architecture ***built*** **to share**.

**That is tough!**”

# Our globally inclusive cyber security ecosystem (where each part can stand alone)



***Secure Realtime Quick-to-Market***

***SR Revolution***

***TruSIP***
*Privacy and Safety Enhanced Computer*

Roaming access with smart card secured ID's

*short range wireless*

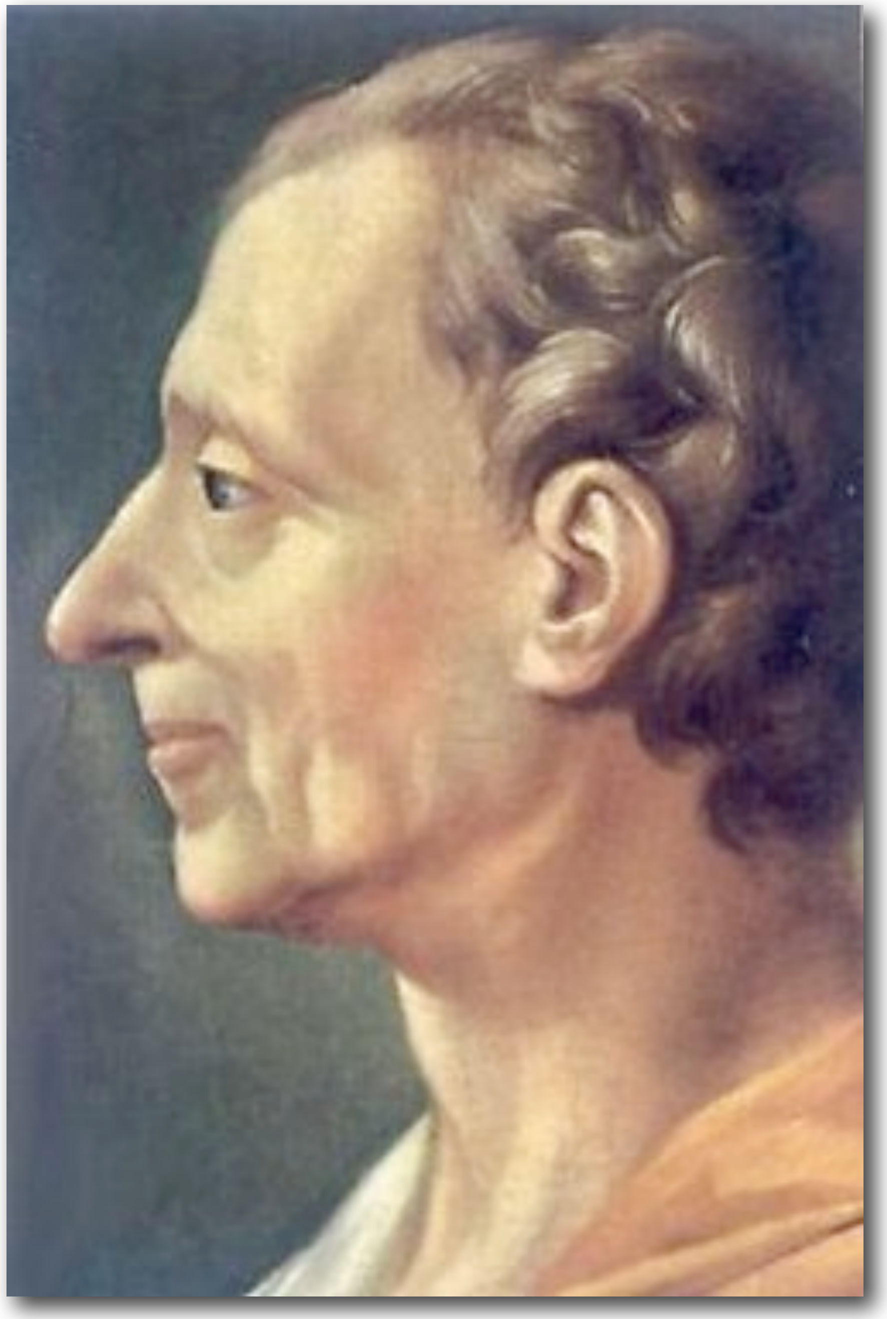
***Global-scale Identity and Key Management***

***Cloud IdM and CKM Service***

***Universal Network Carrier (Janelda)***

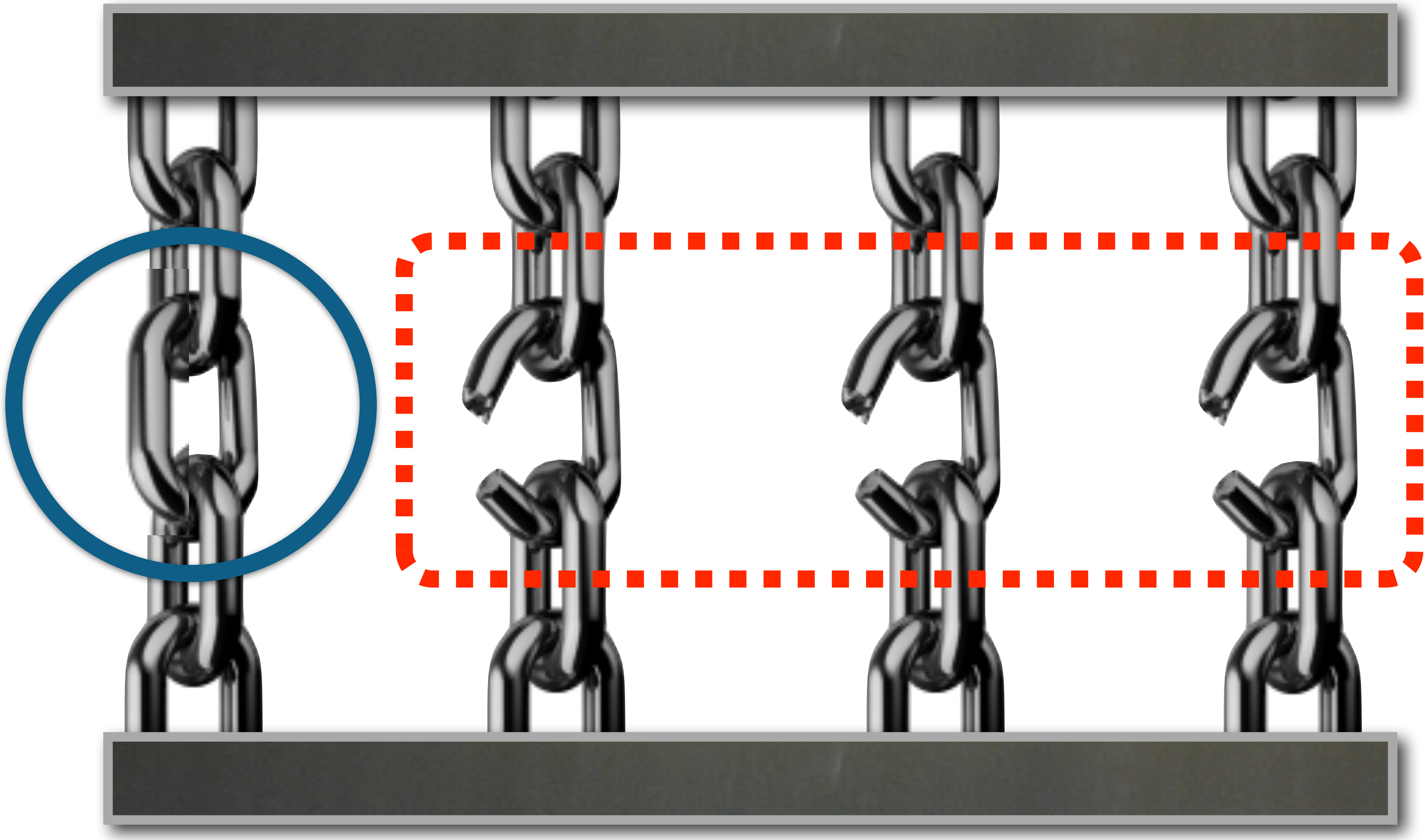
# Our ecosystem will reduce fear

- **Synaptic Labs ICT vision is guided by democratic principles of ‘Spirit of Laws’**
  - Treatise on political theory (1748)
  - Advocated:
    - **separation of powers**
    - **a system of checks & balances**
    - **preservation of civil liberties**
  - Goal:
    - **Enable citizens to have confidence/trust/ assurance in the integrity of the political system**



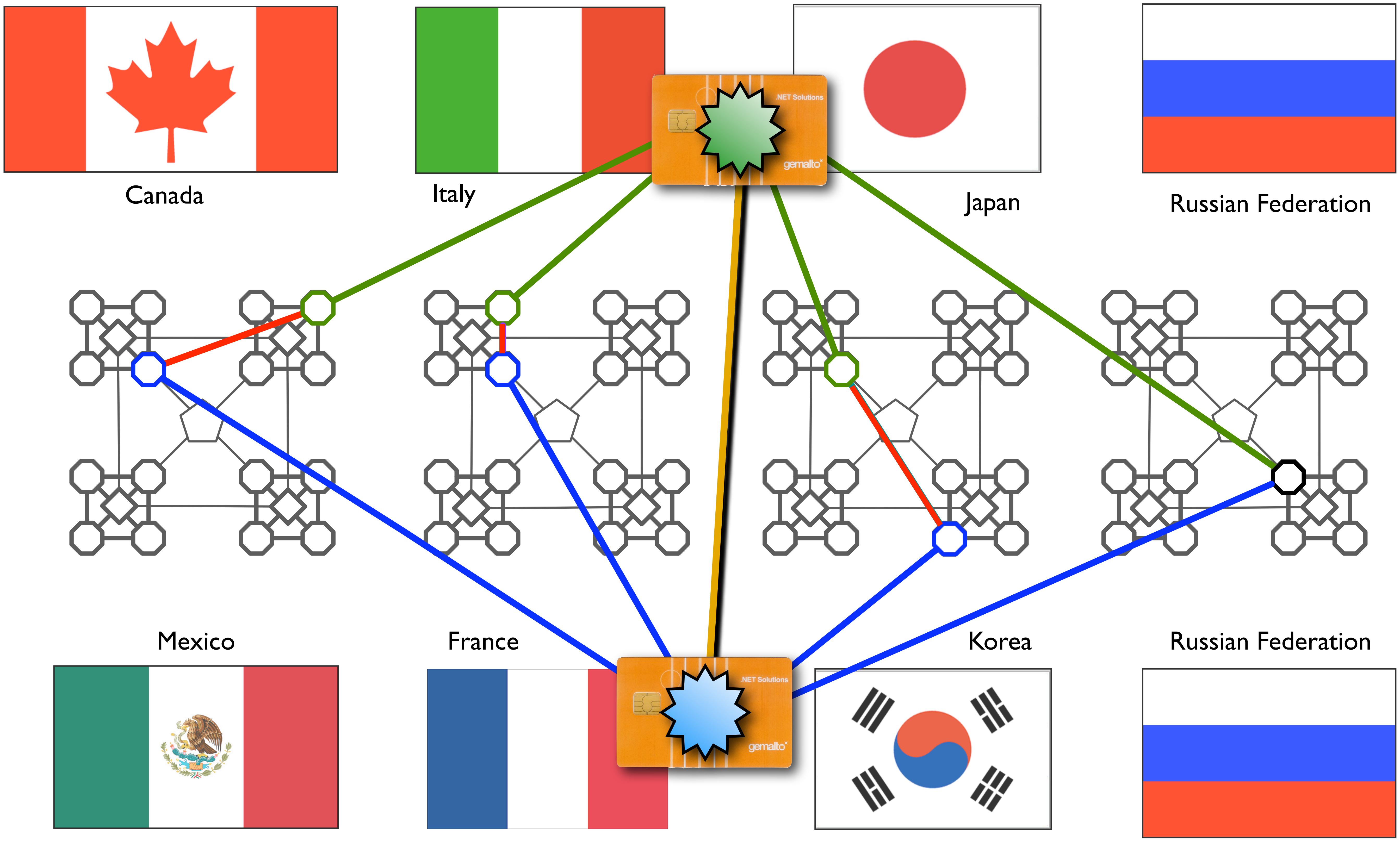
- **Designing these principles more strongly into ICT systems to enable stakeholders to have confidence and trust in specifications, products, services and managers**

# We distribute the burden of trust to reduce fear



- **Each chain represents actions of a sovereign** *(or group of sovereigns)*
  Honest action by one sovereign is sufficient to ensure security
- **For each client transaction, distribute trust across sovereigns**

# This trust model can scale globally...



# We must change our toxic environment!

**“We should also support and get involved in forward-leaning efforts,**

**such as those proposed by Synaptic Laboratories within the ICT Gozo Malta Project.**

They seek to holistically address the hard security problems!

This must be taken on by others as well.”

**Brian Snow**
Public Statement of Support
November 2011

# Advisors and/or Expert Reviewers from...

Green Hills SOFTWARE

OAR RTEMS

OAK RIDGE National Laboratory

CLEMSON UNIVERSITY

WIND RIVER

THALES RESEARCH & TECHNOLOGY

HITACHI Inspire the Next

AEROFLEX GAISLER

AdaCore The GNAT Pro Company

WITTENSTEIN

T-Kernel

ANAGRAN

D:wave

Brian Snow

Tidorum

Entrust®

CYGNACOM SOLUTIONS

Laboratoire PRISM

UT TENSIO SIC VIS

ÉCOLE POLYTECHNIQUE MONTRÉAL

TeZzaron SEMICONDUCTOR

AbsInt

SYNAPTIC
LABORATORIES LTD.

# ICT Gozo Malta

| | | |
|---|---|---|
| Contact: | **Benjamin GITTINS** | |
| | Chief Technical Officer<br>Synaptic Laboratories Limited | Chief Technical Officer<br>ICT Gozo Malta |
| Email: | cto@pqs.io | |
| Phone: | +356 9944 9390 | |
| Web: | www.synaptic-labs.com | www.ictgozomalta.eu |