CNMV
COMISIÓN NACIONAL DEL MERCADO DE VALORES

Sesión 3

TECNOLOGIA EN LOS MERCADOS DE VALORES

FINTECH Y
LA EXPERIENCIA DE SUPERVISAR LAS NORMAS DE CONDUCTA

Jean-Paul Servais
Presidente de la FSMA de Bélgica,
Vicepresidente del Consejo de IOSCO y
Presidente del Comité de Protección del Inversor e Intermediarios de ESMA

FinTech and conduct rule supervisor experience

CNMV – International seminar on the latest developments
on the new securities markets regulations

FSMA

FINANCIAL SERVICES AND MARKETS AUTHORITY

Jean-Paul Servais

Chairman FSMA

Vice-Chairman IOSCO

Chair of ESMA's Financial Innovation Standing Committee

September 20, 2016

Outline

1. FinTech?
2. Challenge for the sector
3. Challenge for the supervisor
4. Approach
5. Some examples

1. FinTech? (I)

IOSCO

"*A traditional interpretation may posit fintech as referencing technology used by incumbent financial institutions to make financial systems more efficient and user friendly (…). More recently the term fintech has come to represent a whole new industry, one that transcends banking to touch all areas of securities markets. This evolution is being driven by the increasing reliance of market participants on online networks, and the introduction of a whole new class of technologies*"

1. FinTech? (II)

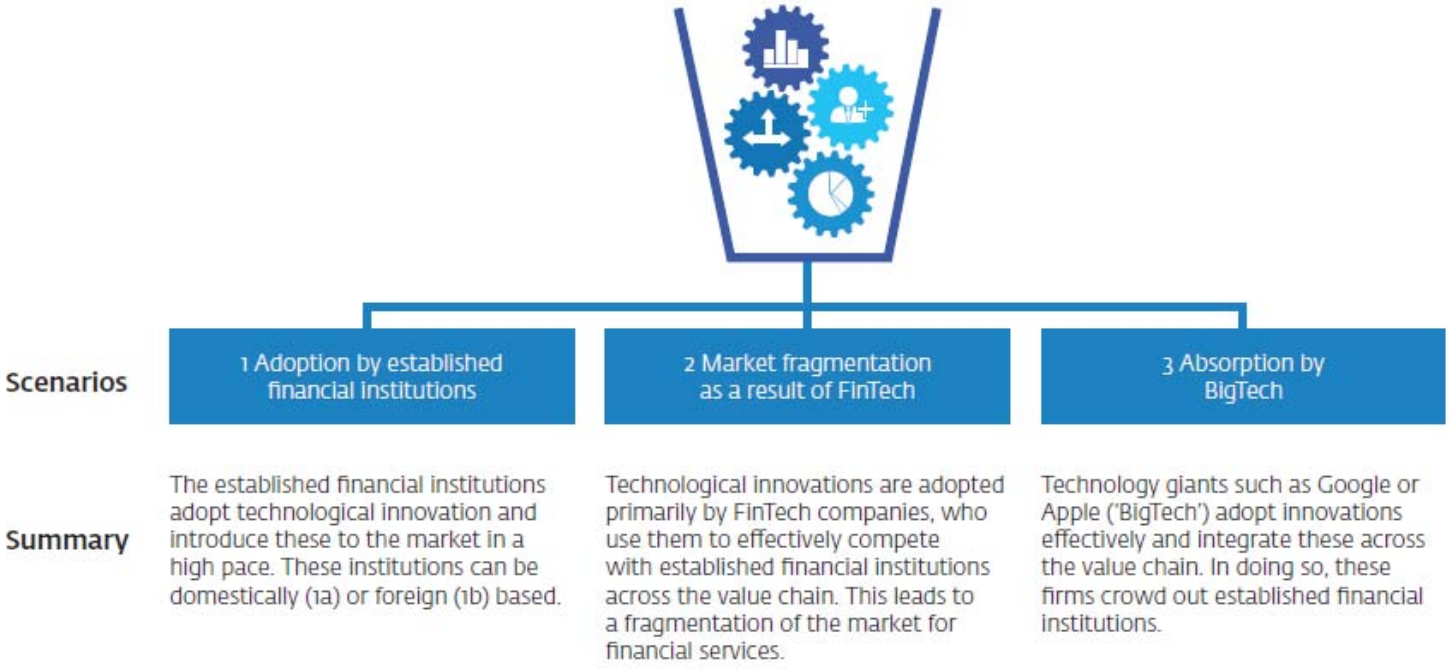
There is no such thing as a FinTech

Examples include:

- Alternative platforms (crowdfunding)
- Digital Ledger Technology / Blockchain
- High frequency trading
- Robo-advice
- Use of Big Data in Banking and Insurance / Internet of Things
- RegTech
- CyberTech
- Payments

2. Challenge for the sector

- **The three scenarios**



Source: *Technological Innovation and the Dutch Financial sector*, DNB, 2016

3. Challenge for the supervisors (I)

- **What are we talking about?**
  - Many ideas…
  - … several of them still need to materialize
- **Issues can be different**
  - Innovation to improve regulated services?
  - Innovation to create new services?
  - Innovation to challenge regulated entities?
- **Who are we talking to?**
- **Keep in mind**

3. Challenge for the supervisors (II)

- **What are we talking about?**
  - Crucial to understand the service at stake in order to be able to
    - qualify it: is it a regulated service or not?
    - identify potential risks linked to either the service as such or the way it is provided
- **Issues can be different**
  - If innovation helps to improve a regulated service, apply current legislation
  - How to approach innovation that creates new services?
    - see the crowdfunding example: ad hoc approach seems needed to avoid hampering the development of such innovation

3. Challenge for the supervisors (III)

- **Who are we talking to?**
  - Dealing with regulated firms is not the same than dealing with FinTech start-ups
  - Intensify contacts
- **Keep in mind**
  - EU directives and regulations
    - MiFID conduct of business requirements are « technology neutral »
    - However, it seems important to verify if those requirements adequately take into account all the aspects of innovation or if some specific additional requirements might be needed (for example, should specific requirements exist regarding the algorithms used when providing robo advice?)
  - Different Members States, different situations

4. Approach

- **Belgium's experience**
  - FSMA's FinTech portal
- **FinTech is on the agenda at European (ESAs, Joint Committee, ECB) and International (IOSCO, BIS, FSB) levels**
  - FinTech is a clear trend and doesn't know frontiers
  - Important to assess together and learn by exchanging
- **ESMA's Financial Innovation Standing Committee**
  - Core task: monitoring and pre-assessment of innovation
  - Permanent topic in FISC agenda
  - Inform ESMA BoS members of potential implications of innovation for supervision
- **Balance between consumer protection and FinTech development**
  - Crowdfunding: pragmatic and reactive

5. Robo advice (I)

- FinTech firms are designing automated tools to meet different customer needs: financial planning, product information, fund management, …
- Automated advice tools can be used to provide advice on a fully automated basis or as a tool for a human advisor to use
- Currently small share of customer assets advised/managed by automated tools but strong growth
- Significant interest and investment from large established firms suggests large market growth ahead

Recent work

- Joint Committee Discussion Paper on automation in financial advice published in Dec 2015 by the three ESAs

5. Robo advice (II)

Possible risks

- May be harder to assess customer understanding without a human to guide through the process
- Algorithms may miss relevant information
- Impact of errors (speed of propagation and number of clients impacted)
- Increasing exposure to IT/ cyber security risks

Possible benefits

- New choices:
  - Possibility to meet different customer needs (e.g. 24/7 access to advice)
  - May increase access to advice, as well as to a wider range of advisers, including facilitating cross-border business
- Lower charges:
  - Lower costs, new entrants, new business models, greater access to some more standardised products
  - Hence more **financial inclusion**

Example of possible challenge for supervisors

- Ensuring consumers understand and are aware of the decisions they are taking

5. Distributed Ledger Technology (I)

- Distributed ledger: sequential 'blocks' of transaction records, automatically verified and stored across a network
- Initial focus on virtual currencies
  - Bitcoin in particular has significant secondary market
- Increasing focus on DLT for market and banking infrastructures
  - Scope to change how data is recorded, shared and agreed across capital and securities markets
  - Could make clearing and settlement quicker and more streamlined
  - Firms will need to move to common standards

<u>Recent ESMA work</u>

- Active area of work for ESMA. Call for evidence published in April 2015; Discussion Paper launched on 2 June 2016
- Dedicated TF set up by FISC

5. Distributed Ledger Technology (II)

Risks

- Trust may be hard to achieve given conceptual complexity
  - Except in one recent case (Ether), DLT has not been hacked
- Fraud or errors
- Scalability not yet proven
- Privacy and governance issues
- Regulatory and legal issues (for example: legality and enforceability of the records?)

Benefits

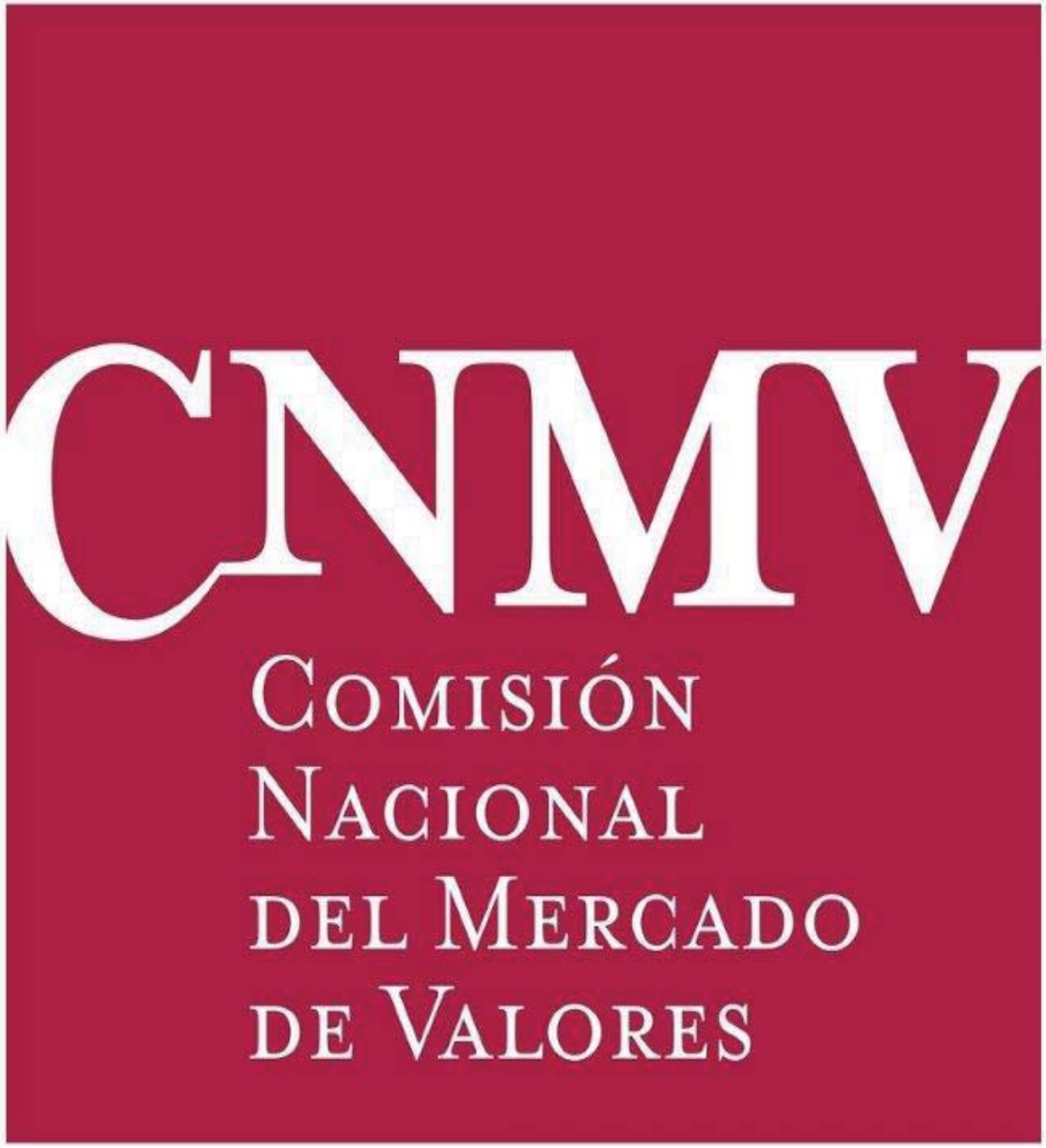
- Speed (instantaneous?)
- Lower costs
  - Reduced need for third parties
  - Less administration
- Transparency
- Security

Example of possible challenges for supervisors

- Building sufficient technical expertise within authorities to assess and scrutinise developments
- Coordinating diverse approaches across firms and countries

Conclusions

- Regulatory and supervisory responses to FinTech should take account of its **features and drivers**
  - S-shaped adoption pattern and fluidity of innovation suggest it is optimal to take time to conduct in-depth observation and analysis
  - Regulatory dialectic shows that effective regulation of FinTech will require a thorough understanding of its drivers
  - Regulatory dialectic also shows need to understand limits of rulemaking
- **Specific expertise** will be needed for regulators to have effective oversight of FinTech
- Don't forget to keep **consumer at the center**
  - One of the potential benefits of FinTech is financial inclusion
  - Not all consumers are « millennials »
  - Are consumers well equipped to make decisions in a digitalized instantaneous world?
  - Financial education is key


CNMV
Comisión
Nacional
del Mercado
de Valores

CIBER SEGURIDAD

Juan Antonio Gómez-Bule
Presidente del grupo de trabajo en el Centro de Estudios Superiores de Defensa Nacional

Session 3:
SECURITY MARKETS TECHNOLOGIES
CYBERSECURITY

PHRASES TO CONSIDER

“Now this is not the end. It is not even the beginning of the end. But it is, perhaps, the end of the beginning.”
Winston Churchill,1942

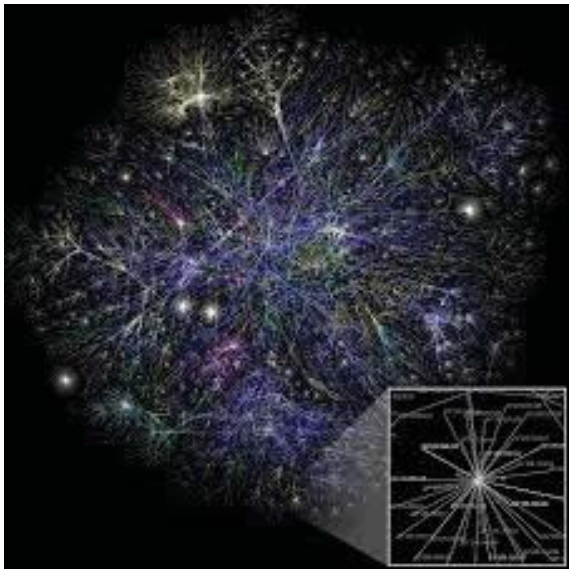
"Everything flows, nothing stays still“
"change is the only constant“
Heraclitus of Ephesus (550-475 BC)

TRUST IN AN HYPERCONNECTED WORLD

"Ultimately, in a highly interconnected and interdependent financial ecosystem, cyber attacks may have systemic implications for the entire financial system, and also affect over time the trust on which financial markets are built. For these and other reasons, regulators, market participants, and other stakeholders must work together to enhance cyber security in securities markets "

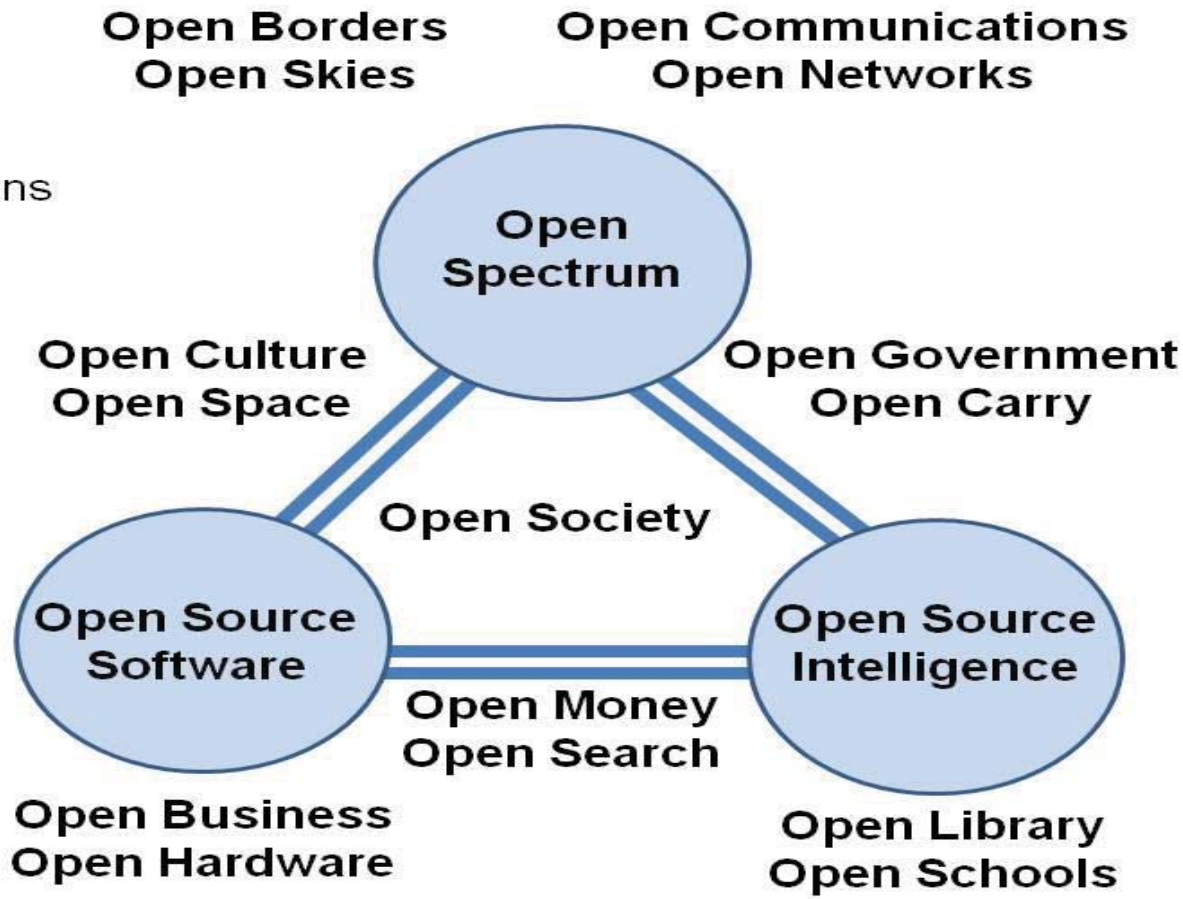
Cyber Security in Securities Markets – An International Perspective

Report on IOSCO's cyber risk coordination efforts

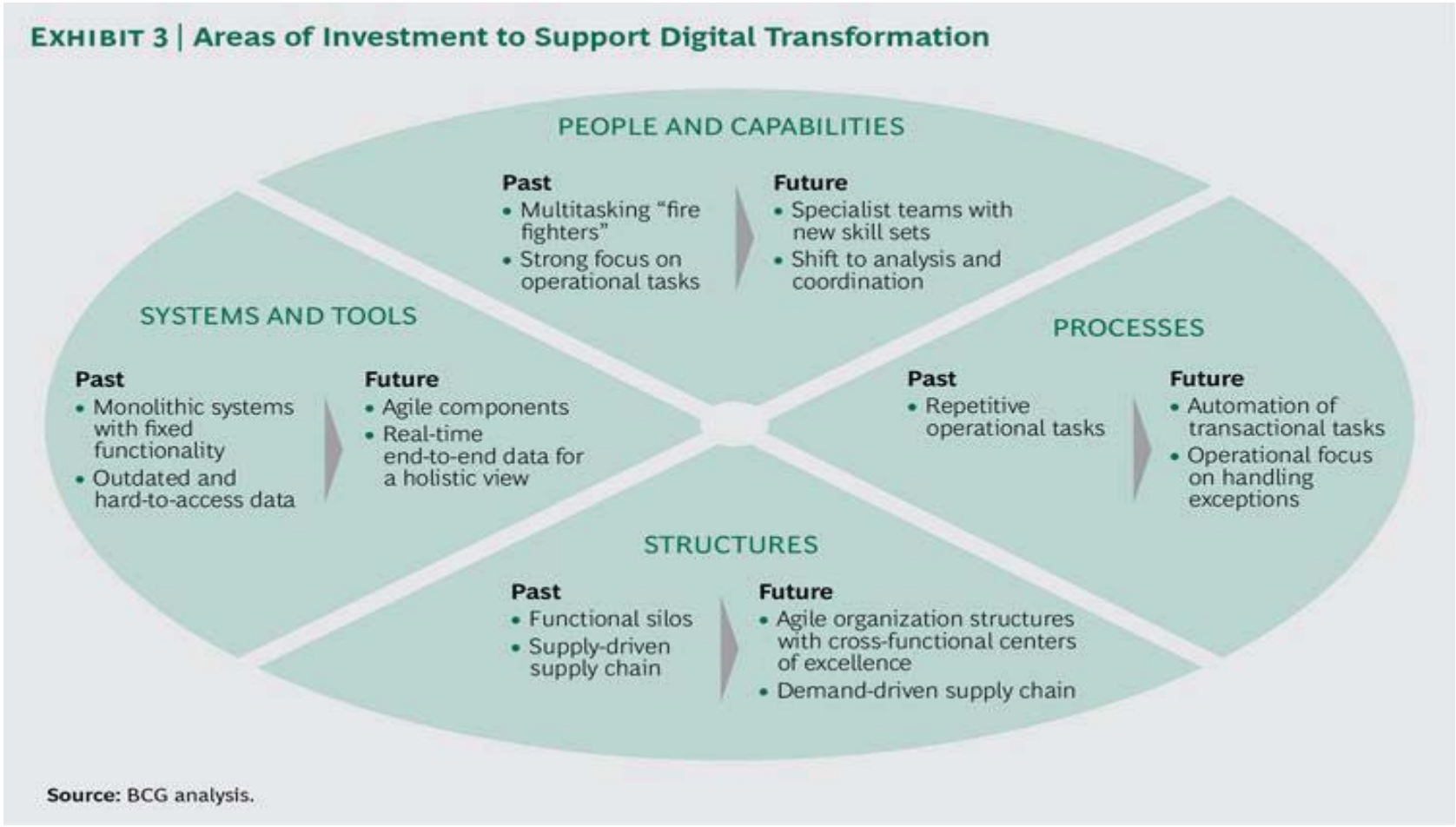


A NEW OPEN AND CHANGING WORLD

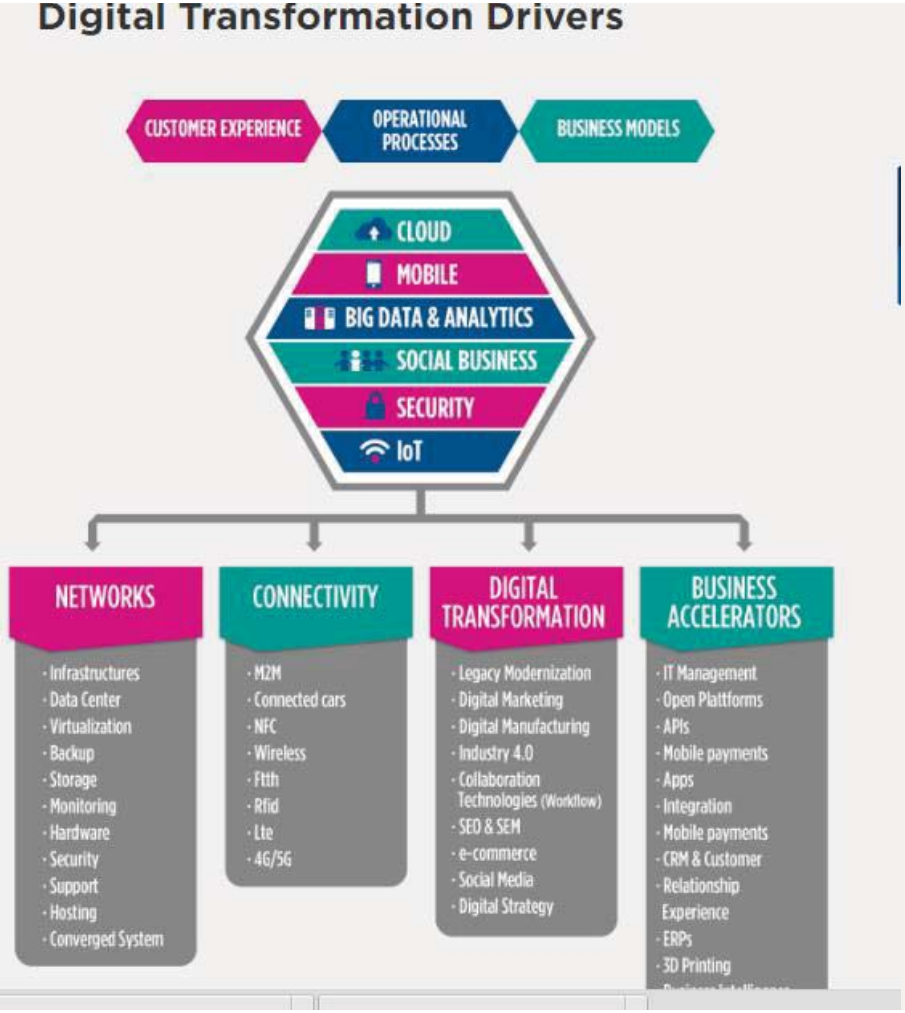
Open Borders
Open Business
Open Carry
Open Communications
Open Culture
Open Government
Open Hardware
Open Intelligence
Open Library
Open Money
Open Networks
Open Schools
Open Search
Open Skies
Open Society
Open Software
Open Space
Open Spectrum
…
…
Open Everything

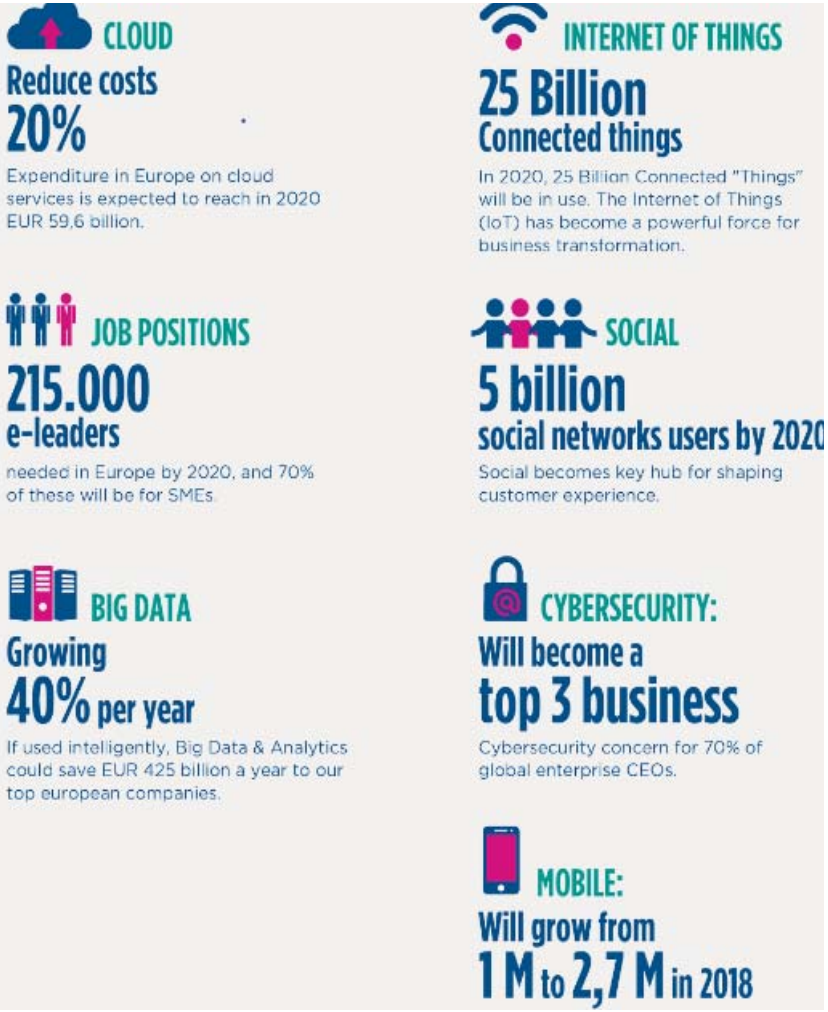


THE SOCIETY´S DIGITAL TRANSFORMATION



THE SOCIETY´S DIGITAL TRANSFORMATION





WEF APPROACH

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The Future of Financial Services

How disruptive innovations are reshaping the way financial services are structured, provisioned and consumed

An Industry Project of the Financial Services Community | Prepared in collaboration with Deloitte

Final Report • June 2015

WEF 2016

WORLD ECONOMIC FORUM Agenda Initiatives Reports Events About TopLink login 中文 Español

Global Agenda › Cyber Security › Fragility, Violence and Conflict

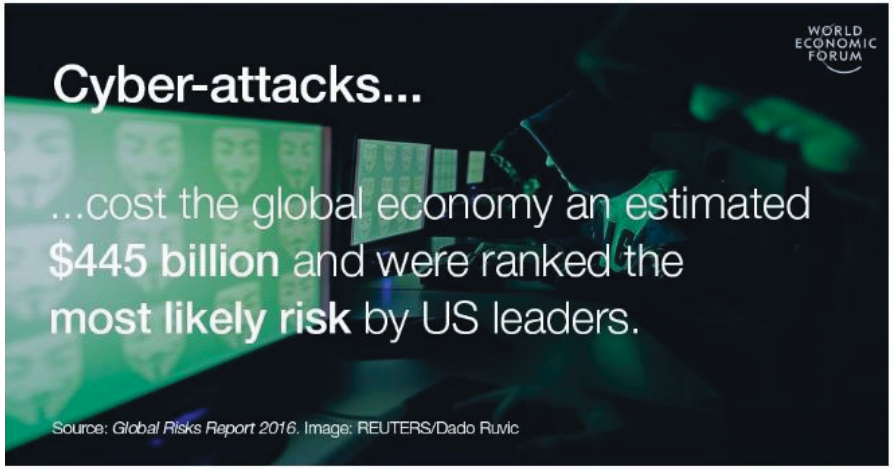
Who are the cyberwar superpowers?

WORLD ECONOMIC FORUM Agenda Initiatives Reports Events About TopLink login 中文 Español

Global Agenda › Cyber Security › Risk and Resilience › Technology

Why should we care about cyber resilience? Because $445 billion is at stake

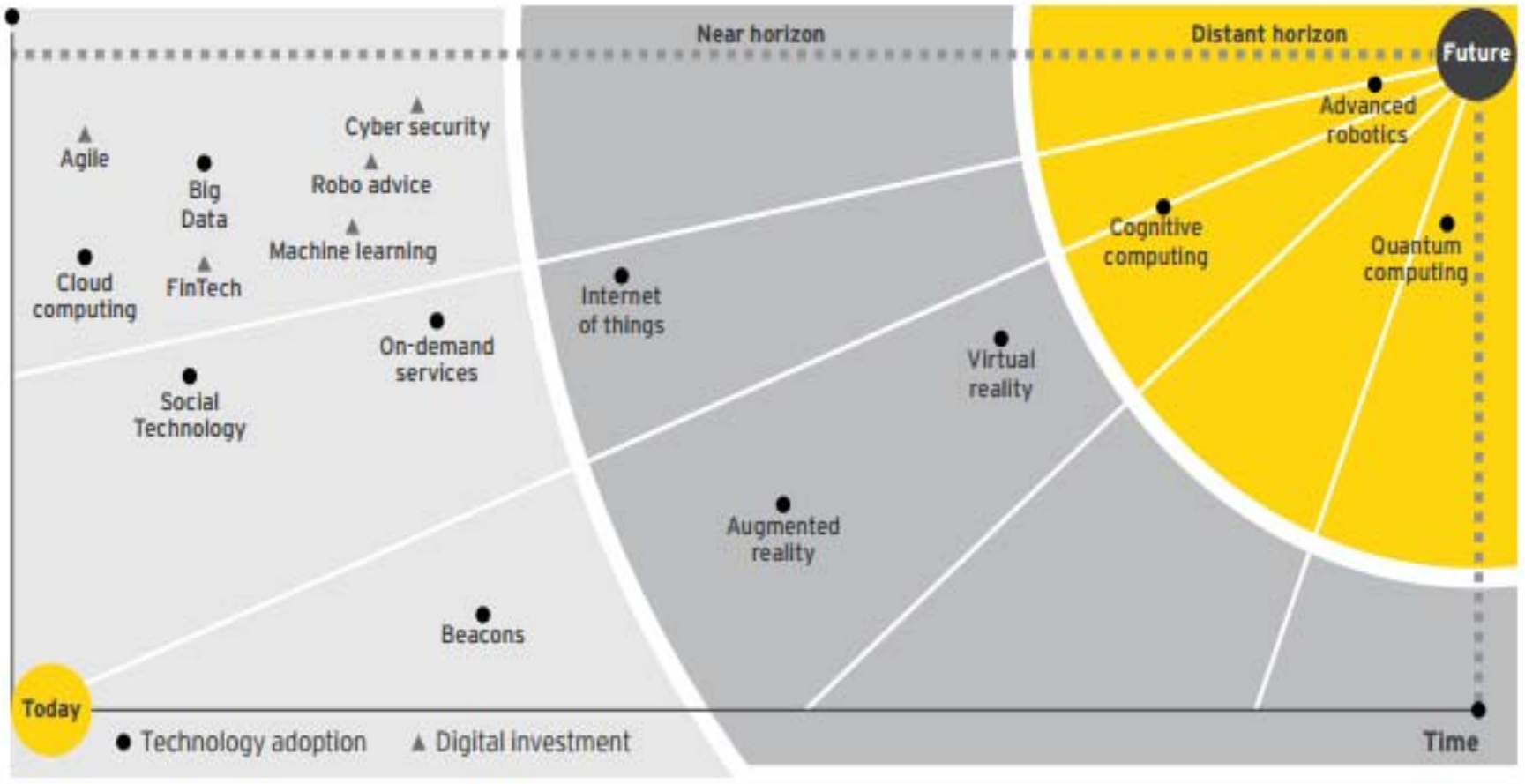
WEF 2016



Ponemon INSTITUTE

2016 Cost of Data Breach Study: Global Analysis

TECHNOLOGIES TRENDS APPLIED IN BANKS

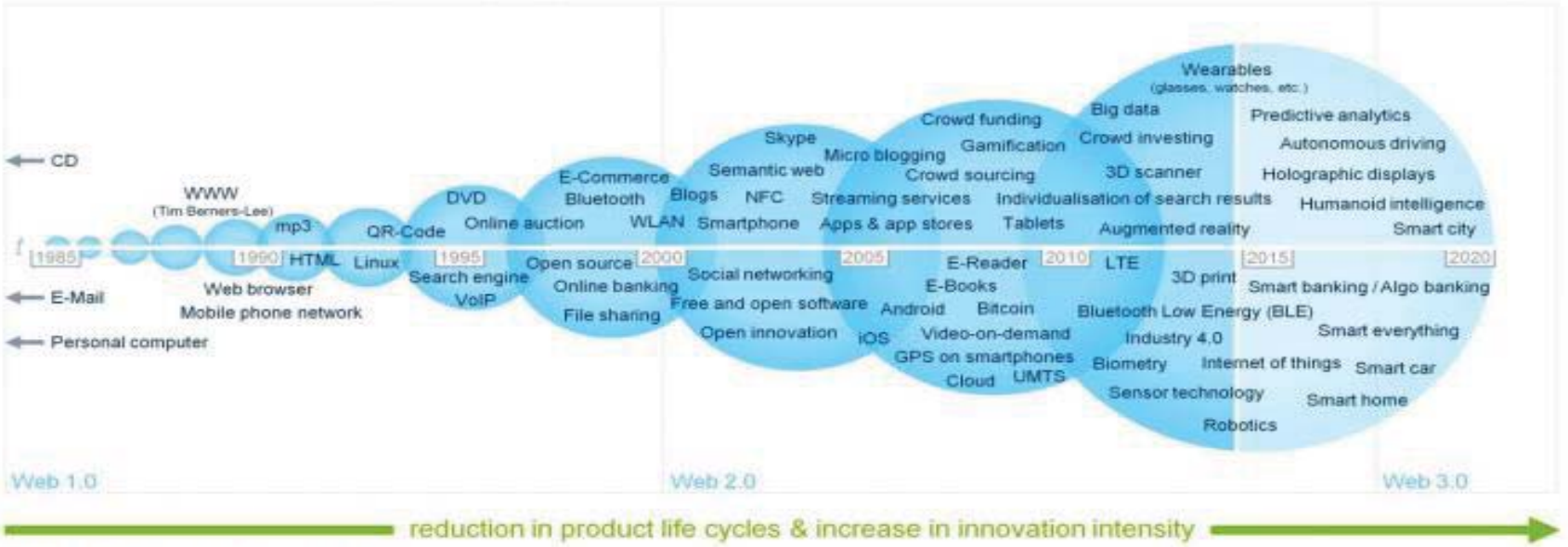


FINTECH THE DIGITAL REVOLUTION

Deutsche Bank
Research

Fintech – The digital (r)evolution in the financial sector

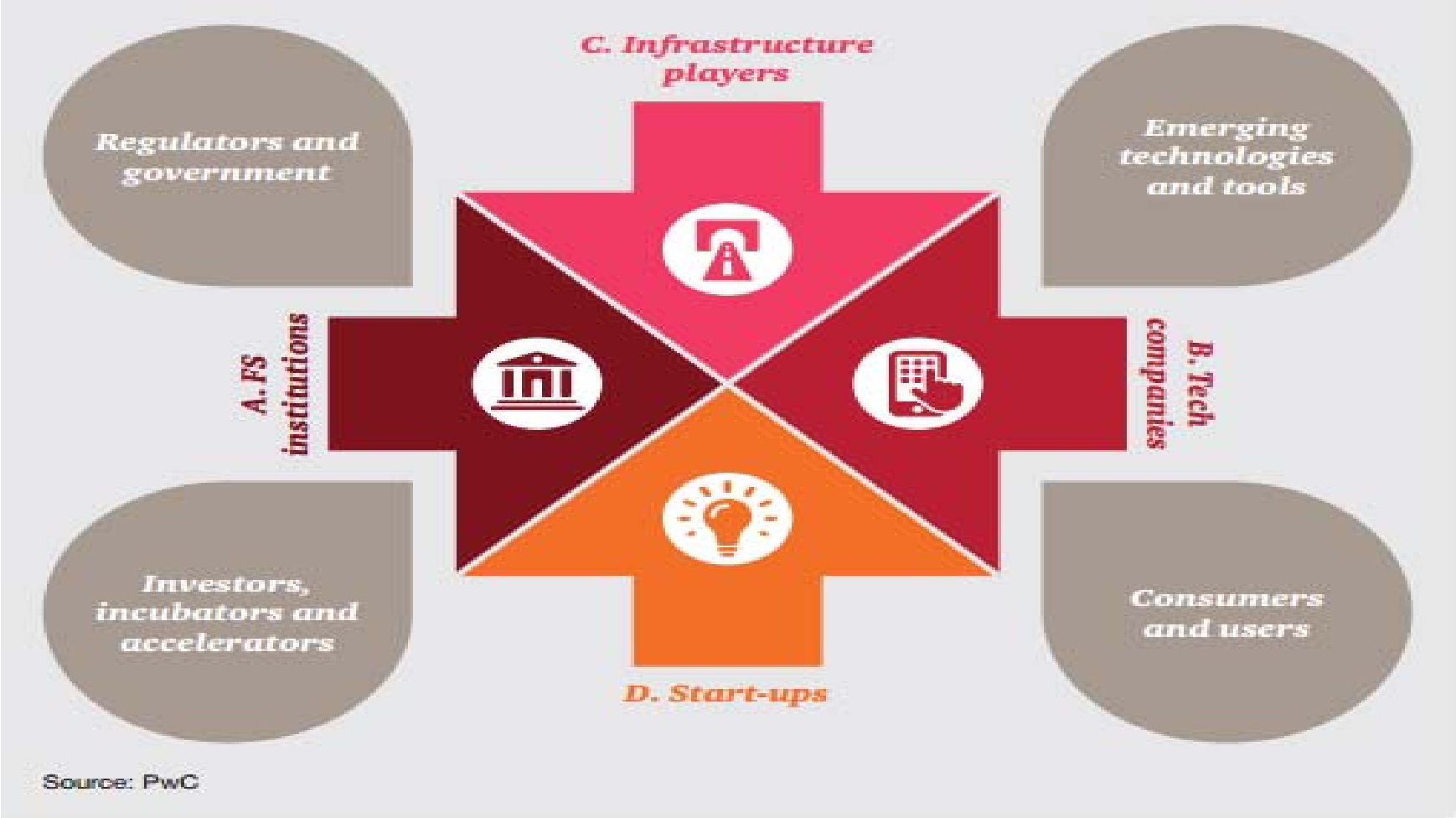
Milestones in the internet age 6



Graph: Oliver Ullmann. Deutsche Bank Research.

Source: Dapp, T. (2014). Fintech – The digital (r)evolution in the financial sector: Algorithm-based banking with the human touch. Deutsche Bank Research. Frankfurt am Main.

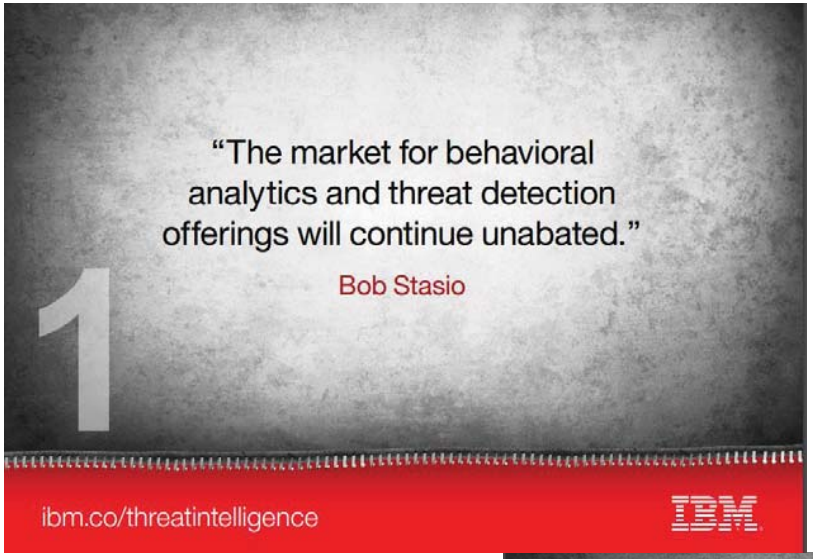
FINTECH IS A COMPLEX SYSTEM



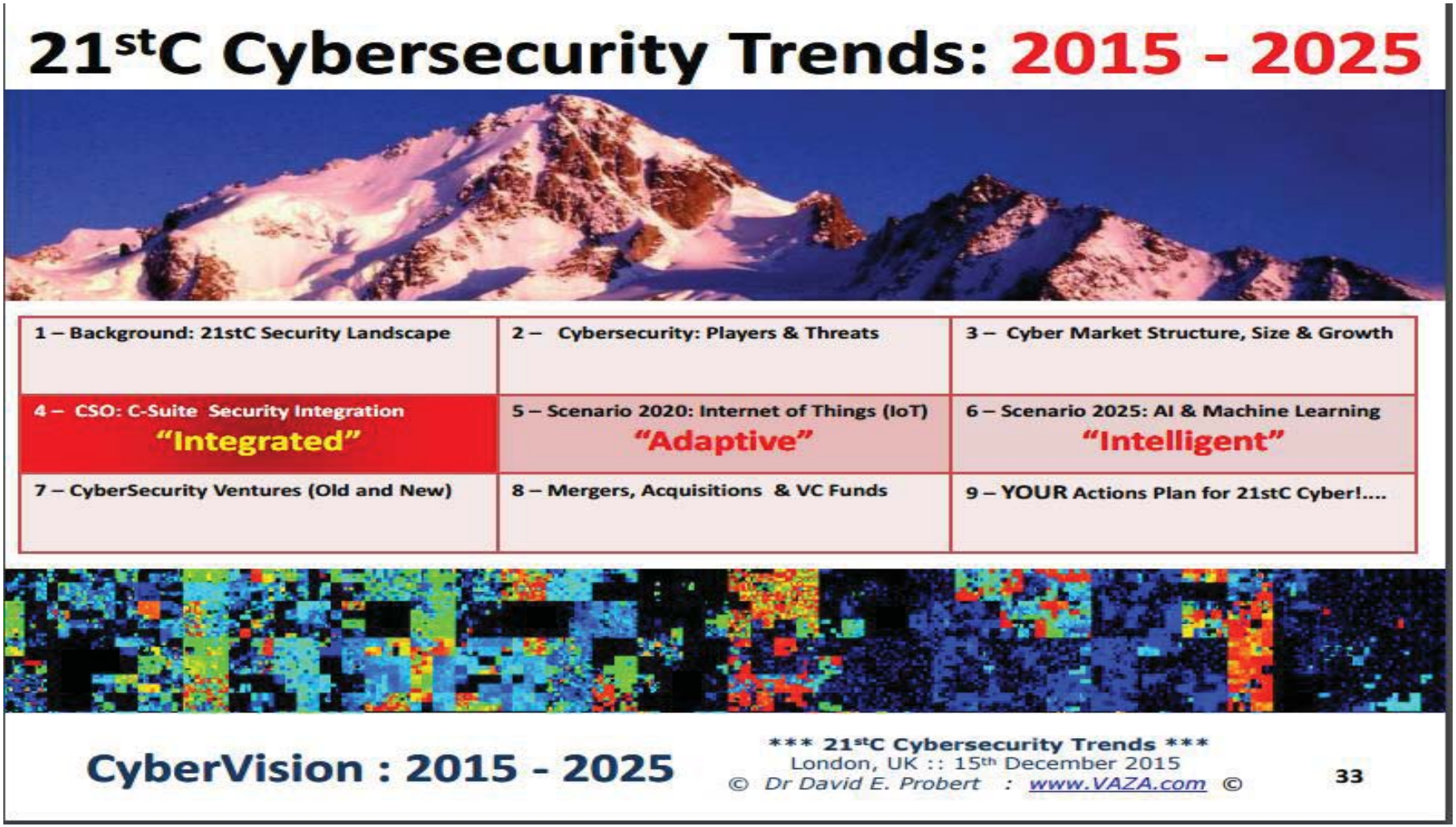
BLOCKCHAIN AND CYBERSECURITY

By removing the need for a middleman, blockchain also enhances security. The more parties involved in a transaction, the greater the risk that one could be compromised. But in a blockchain network, transactions happen directly between parties, so there's less chance of failure at one of the handoff points.

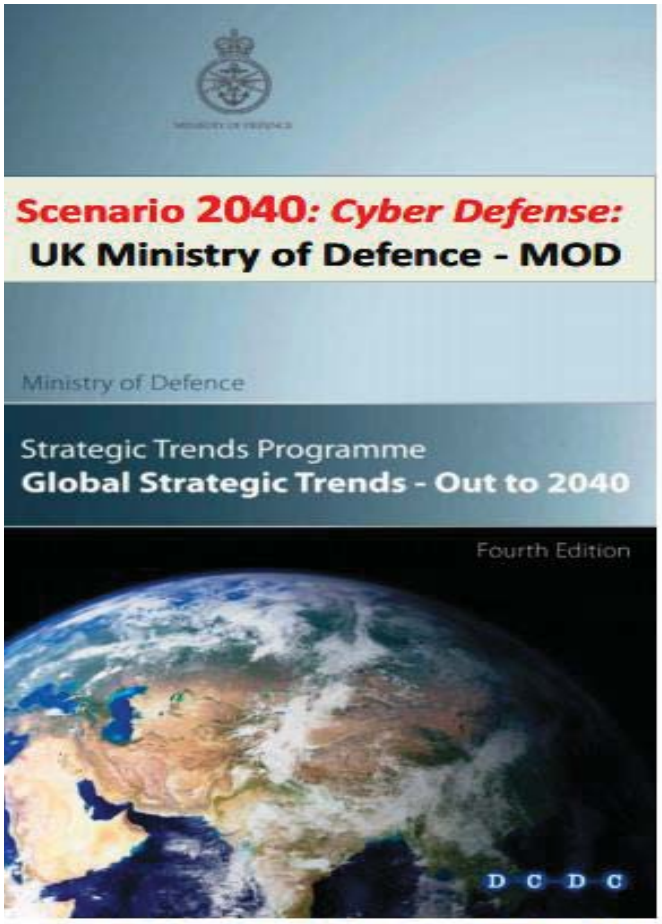
MARKETS TRENDS IN 2016 BY IBM

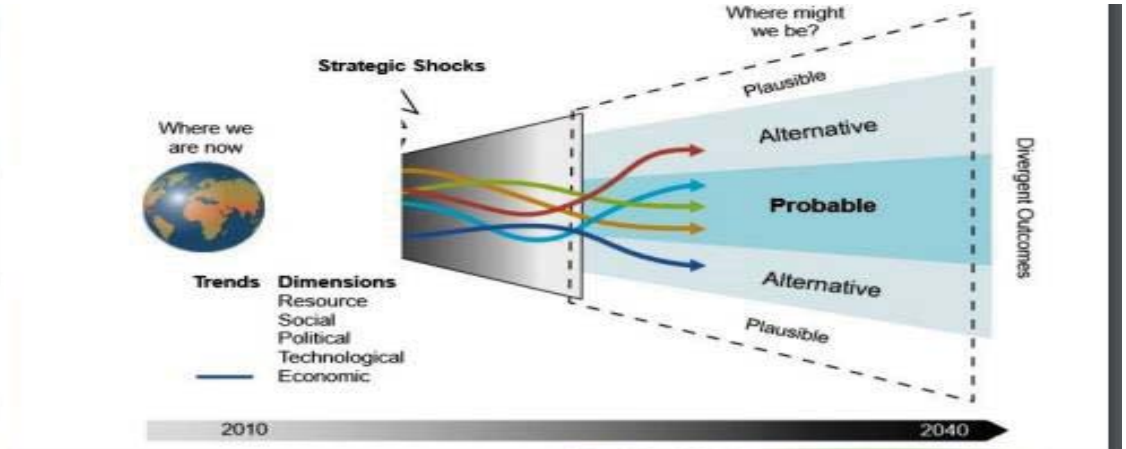


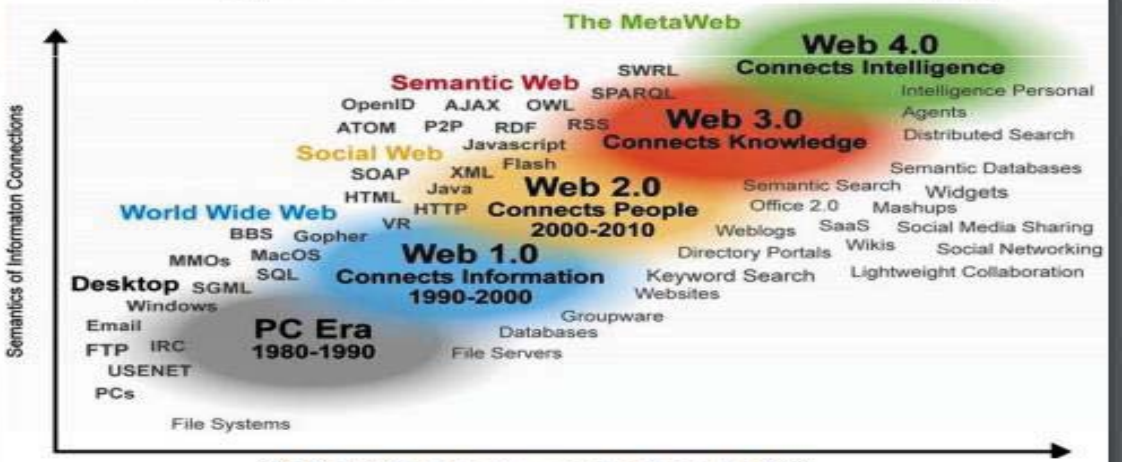
CYBERSECURITY TRENDS



CYBERSECURITY TRENDS







CyberVision : 2015 - 2025

*** 21stC Cybersecurity Trends ***
London, UK :: 15th December 2015
© Dr David E. Probert : www.VAZA.com ©

CYBERSECURITY INVESTMENT

Forbes / Tech

The Little Black Book of Billionaire Secrets

MAR 9, 2016 @ 07:24 AM 3,151 VIEWS

Worldwide Cybersecurity Spending Increasing To $170 Billion By 2020

Steve Morgan, CONTRIBUTOR

I write about the business of cybersecurity.

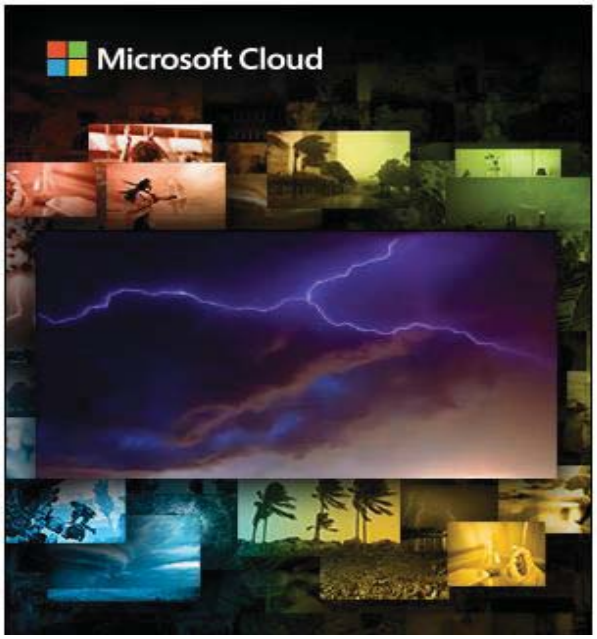
FOLLOW ON FORBES (24)

Opinions expressed by Forbes Contributors are their own.

FULL BIO

The Wall Street Journal Venture Capital Dispatch is the latest to cite research from Gartner, Inc. which reports the world-wide cybersecurity market topped $75 billion in 2015.

"Interest in security technologies is increasingly driven by elements of digital business, particularly cloud, mobile computing and now also the Internet of Things, as well as by the sophisticated and high-impact nature of advanced



CYBER RESILIENCE FOR FINANCIAL MARKET INFRASTRUCTURES (IOSCO)

- Sound cyber governance is key. Board and senior management attention is critical to a successful cyber resilience strategy.
- The ability to resume operations quickly and safely after a successful cyber attack is paramount.
- FMIs should make use of good-quality threat intelligence and rigorous testing.
- FMIs should aim to instil a culture of cyber risk awareness and demonstrate ongoing re-evaluation and improvement of their cyber resilience at every level within the organisation.
- Cyber resilience cannot be achieved by an FMI alone; it is a collective endeavour of the whole "ecosystem".

GLOBAL ECONOMIC CYBERWARFARE

HOME | PREVIOUS POSTS

SUBSCRIBE

GLOBAL ECONOMIC WARFARE
RISKS & RESPONSES

Cyber Warfare is Here. Are We Prepared? Or Are Our Heads in the Sand?

by KEVIN D. FREEMAN on JANUARY 19, 2015

SUBSCRIBE

Receive notifications of new posts by email.

Email Address

Subscribe

LINKS

www.SecretWeapon.org

RECENT POSTS

The Law of Unintended Consequences Strikes Again...

WHY ATTACK ONE CRITICAL INFRASTRUCTURE?

National Security

- Reduce the ability to protect its interests

Public Psyche

- Erode confidence in critical services and the government

Economic impact

- Damage economic systems

Enhancement of Physical Attacks

- Physical damage/distraction efforts

Asymmetric Warfare

- Lack of attribution, low cost/high potential impact

CYBERTERRORISM

Is a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda.

- Cyber intelligence and forensics to counter terrorism and cybercrime
- Threat identification and impact evaluation systems
- Cyber resilience for critical infrastructure

CYBERTERRORISM

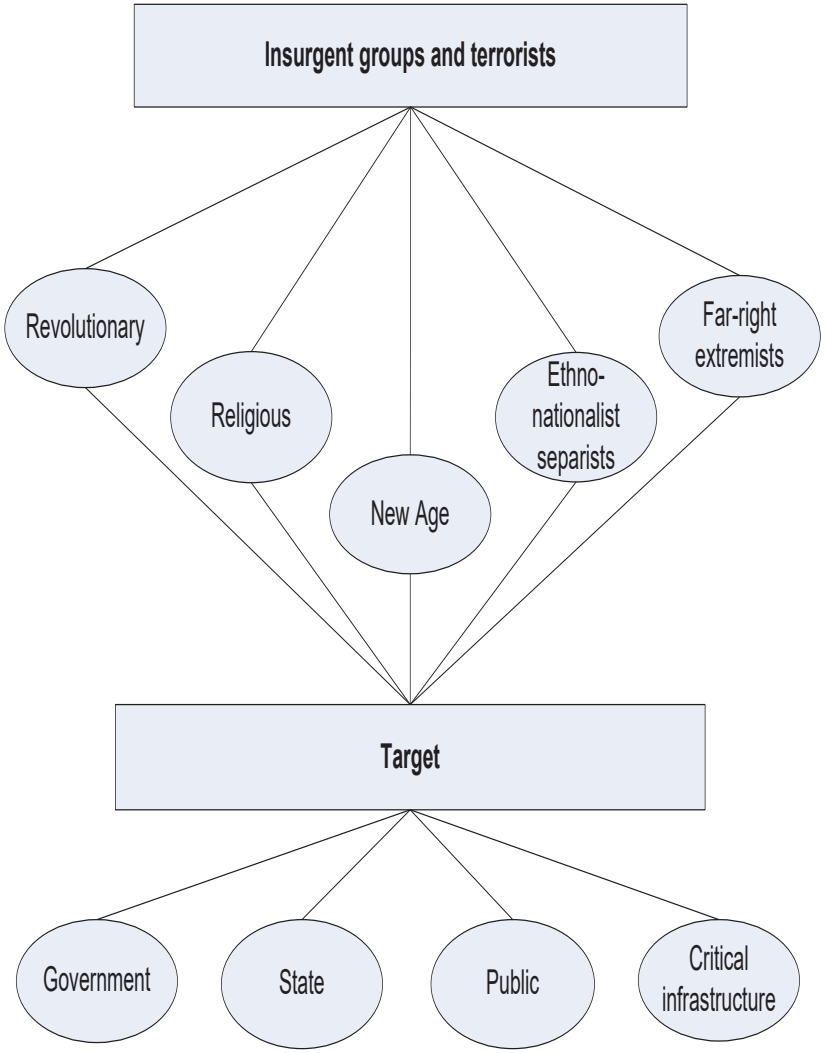
Cyberspace potential means through which terrorists could cause chaos

Affect psyche of communities

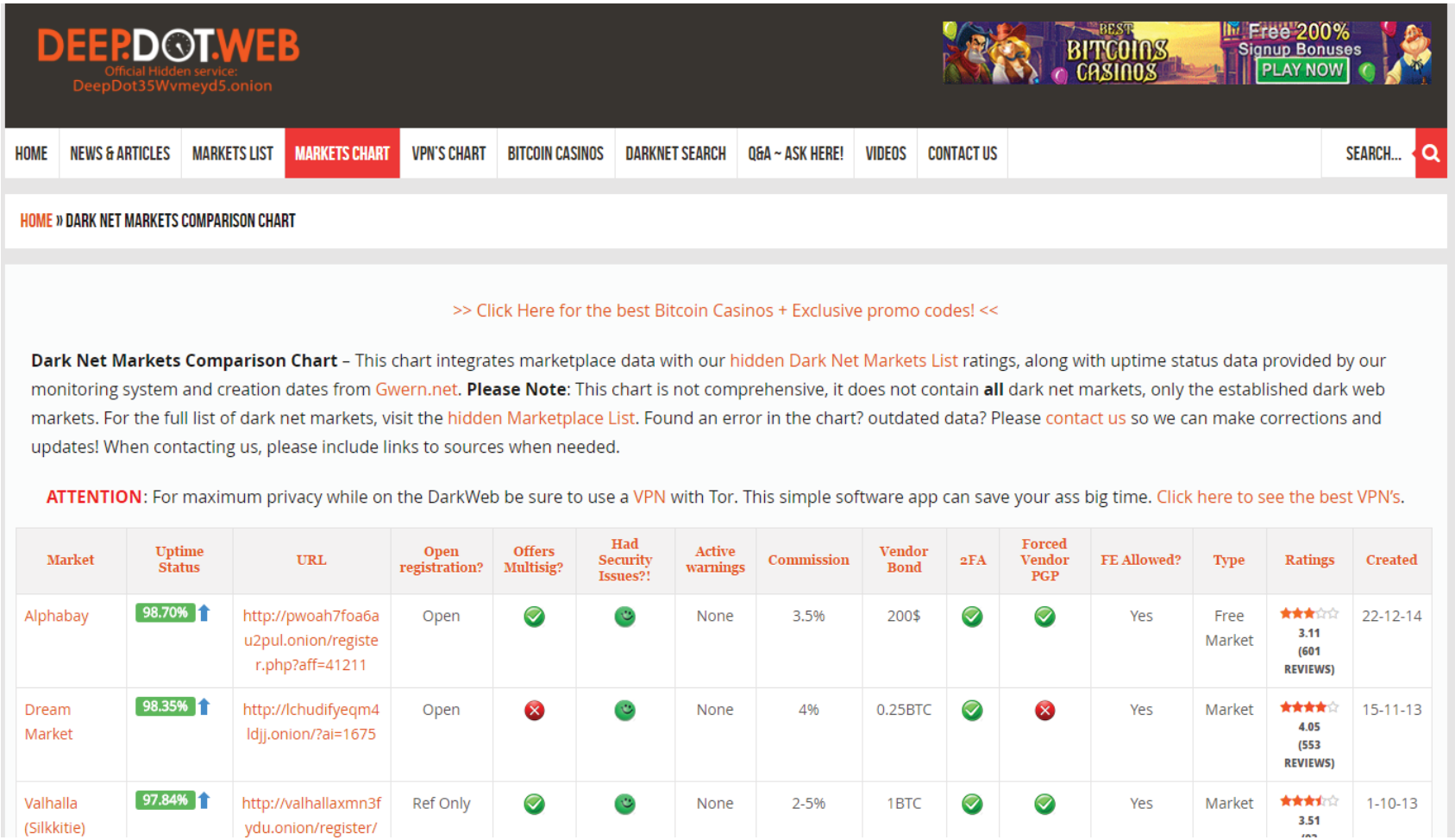
Underlying political, social, religious reasoning for violent and extremist behaviour

Summary of political, religious, legal, economic, social and technical issues to combat

Include countermeasures likel laws, fusion centres, education, treaties, network monitoring and CSIRTs



CRIME AS A SERVICE MARKETPLACE



DEEP.DOT.WEB
Official Hidden service:
DeepDot35Wvmeyd5.onion

HOME | NEWS & ARTICLES | MARKETS LIST | MARKETS CHART | VPN'S CHART | BITCOIN CASINOS | DARKNET SEARCH | Q&A ~ ASK HERE! | VIDEOS | CONTACT US | SEARCH...

HOME » DARK NET MARKETS COMPARISON CHART

>> Click Here for the best Bitcoin Casinos + Exclusive promo codes! <<

Dark Net Markets Comparison Chart – This chart integrates marketplace data with our hidden Dark Net Markets List ratings, along with uptime status data provided by our monitoring system and creation dates from Gwern.net. **Please Note**: This chart is not comprehensive, it does not contain **all** dark net markets, only the established dark web markets. For the full list of dark net markets, visit the hidden Marketplace List. Found an error in the chart? outdated data? Please contact us so we can make corrections and updates! When contacting us, please include links to sources when needed.

ATTENTION: For maximum privacy while on the DarkWeb be sure to use a VPN with Tor. This simple software app can save your ass big time. Click here to see the best VPN's.

Market	Uptime Status	URL	Open registration?	Offers Multisig?	Had Security Issues?!	Active warnings	Commission	Vendor Bond	2FA	Forced Vendor PGP	FE Allowed?	Type	Ratings	Created
Alphabay	98.70%	http://pwoah7foa6au2pul.onion/register.php?aff=41211	Open	✓	✓	None	3.5%	200$	✓	✓	Yes	Free Market	3.11 (601 REVIEWS)	22-12-14
Dream Market	98.35%	http://lchudifyeqm4ldjj.onion/?ai=1675	Open	✗	✓	None	4%	0.25BTC	✓	✗	Yes	Market	4.05 (553 REVIEWS)	15-11-13
Valhalla (Silkkitie)	97.84%	http://valhallaxmn3fydu.onion/register/	Ref Only	✓	✓	None	2-5%	1BTC	✓	✓	Yes	Market	3.51	1-10-13

DEEP WEB


The part most of us are familiar with. This comprises only 10% of the total size of the internet. All sites are indexed by search engines and are easily accessible.
Examples: Facebook, Twitter, etc
Size: ~19 TB / ~980,000,000 websites
Largely unfiltered and cluttered
10%
90%
SPECIAL ACCESS ONLY AFTER THIS POINT
Deep Web
Refers to the content on the internet that is not indexed by standard search engines. The Deep Web contains mostly innocuous things

DARK WEB


Examples:
Academic information, medical records, legal documents, government resources
Size: ~7,500 TB / Unknown number of sites
Extremely well organised and filtered
100% ANONYMOUS AFTER THIS POINT
Dark Web
The Dark Web forms the deepest layer of the Deep Web. It is believed most of the content here is of a criminal nature.

CYBER EXCELENCE IS A GOAL

CYBER EXCELLENCE

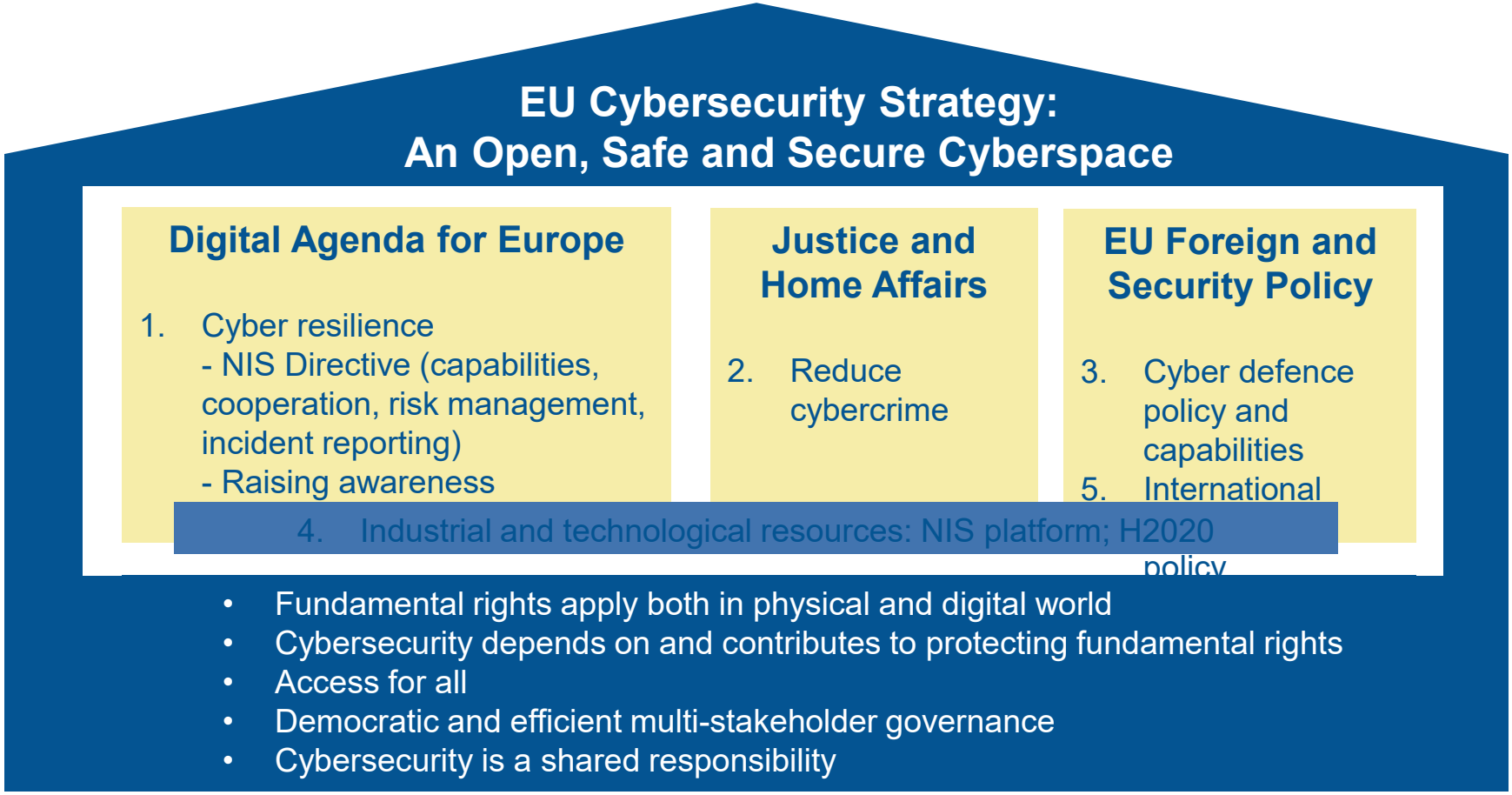
CYBER INTELLIGENCE
UNDERSTANDING & KNOWLEDGE: WHO, WHAT, WHEN, WHERE, HOW

CYBER SECURITY
THE ABILITY TO RAPIDLY RESPOND, MONITOR, & PREVENT

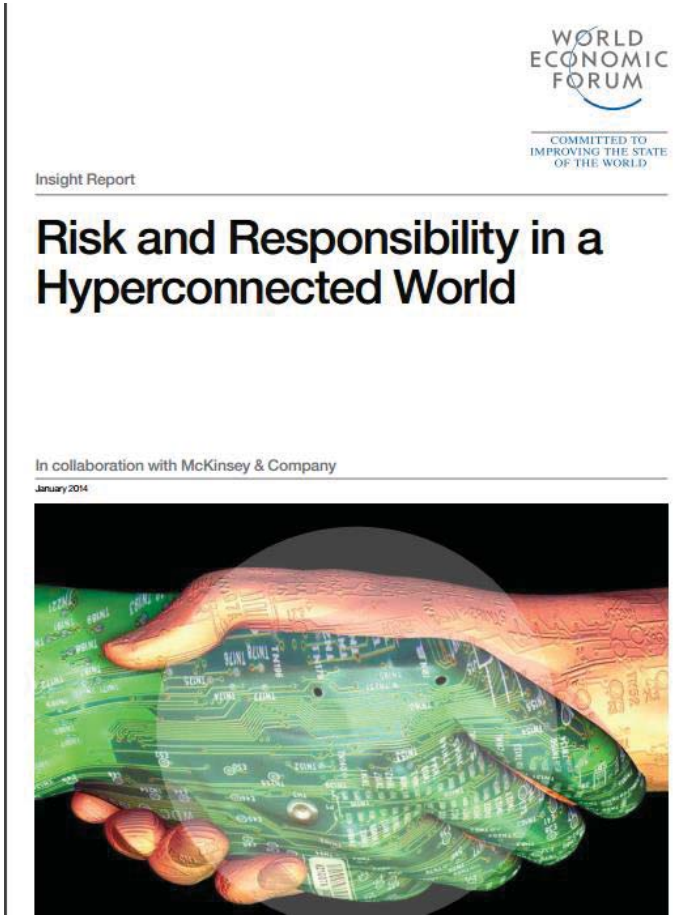
CYBER TRAINING
LESSONS LEARNED & COLLABORATION IMPROVING TOMORROW

CYBER TECHNOLOGY
ENABLING EFFECTIVE APPLICATION

CYBERSECURITY IS A SHARED RESPONSIBILITY



CYBERATTACKS READINESS: FROM FEAR TO CONFIDENCE



Cyber security is not a department, but an attitude Cyber security is often seen as the responsibility of a department of specialist professionals. This mindset may result in a false sense of security and lead to the wider organization not taking responsibility. The real challenge is to make cyber security a mainstream approach

CYBERATTACKS READINESS: FROM FEAR TO CONFIDENCE

1 Institutional readiness	**Governance** Prioritize information assets based on business risks and integrate cyber resilience into enterprise-wide risk management
	Program development Differentiate protection based on importance of assets. Develop deep integration of security into technology environment. Deploy active defenses to uncover attacks proactively. Continuous testing to improve incident response and enlist front-line personnel
	Network development Coordinate better with partners, vendors, and other counterparts to effectively mitigate network risk
2 Public and international policy	**National cyber strategy** Establish a comprehensive, transparent national cyber strategy that integrates procedures across all policy domains
	End-to-end criminal justice system Ensure that law enforcement and the state have a comprehensive and flexible legal code and capabilities to take action
	Domestic policy and incentives Establish private, public, and civil dialogue to develop suitable policy and market mechanisms
	Foreign policy Establish a national cyber strategy. Identify institutions and critical capabilities and harmonize policies through multi-stakeholder collaboration
	Public goods Encourage multi-stakeholder collaboration to invest in capabilities, capacity and resources for the public good
3 Community	**Research** Invest in research to better understand the cyber landscape and threats
	Information sharing Work to promote better information sharing by further developing collaboration tools and resources
	Shared resources for capability building Foster partnerships between governments, universities, and the private sector to develop capabilities and capacity
4 Systemic	**Risk markets** Explore and invest to develop risk markets and value risks from cyber events
	Embedded security Work to better integrate security into current technology systems and tools

GLOBAL IMPACT CYBERSECURITY THREATS

Midyear Review: The Continuing Challenge of Financial Services Threats

June 27, 2016 | By Christopher Burgess

iStock

Looking back on the first half of 2016, we've seen that financial services threats have not dissipated — and they are not anticipated to do so anytime soon. Unfortunately, prognosticating security threats is about as accurate as predicting the weather, except banks of supercomputers do the calculations for meteorologists, while the security analyst is often left with reams of data, instincts and experience. Still, experts try to forecast what's on the horizon to be better prepared when the inevitable issue strikes.

Financial services threats are very real, though not limited strictly to the financial industry. Threat predictions at the beginning of the year touched on nation-states, organized crime, biometric security, credit card fraud, criminal exchanges and crime within the mobile environment.

CYBERSECURITY AND CYBERRISK (DELOITTE)

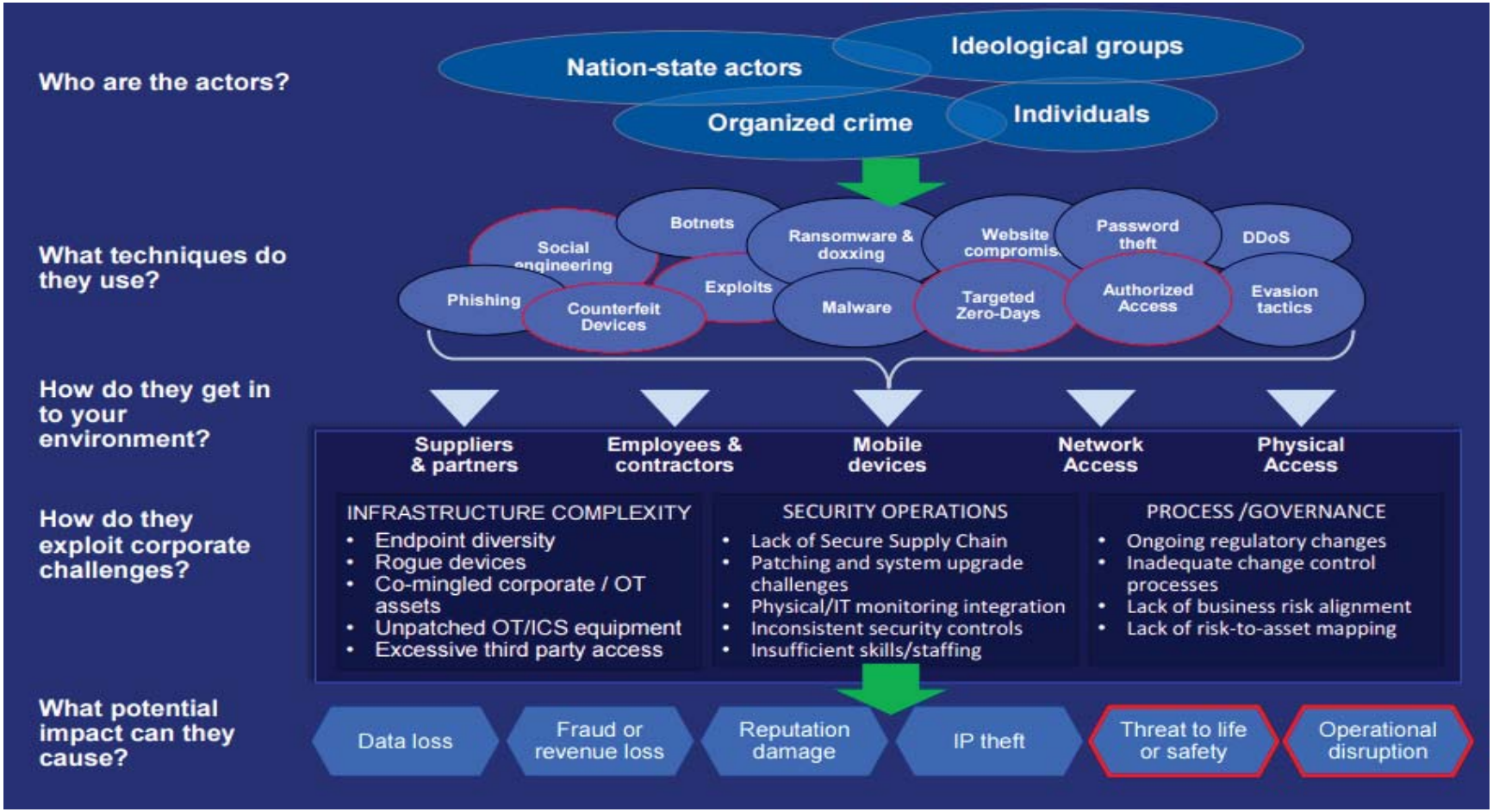
Cyber Risk ≠ Cyber Security

Cyber risk and cyber security are often used interchangeably however they are two different concepts

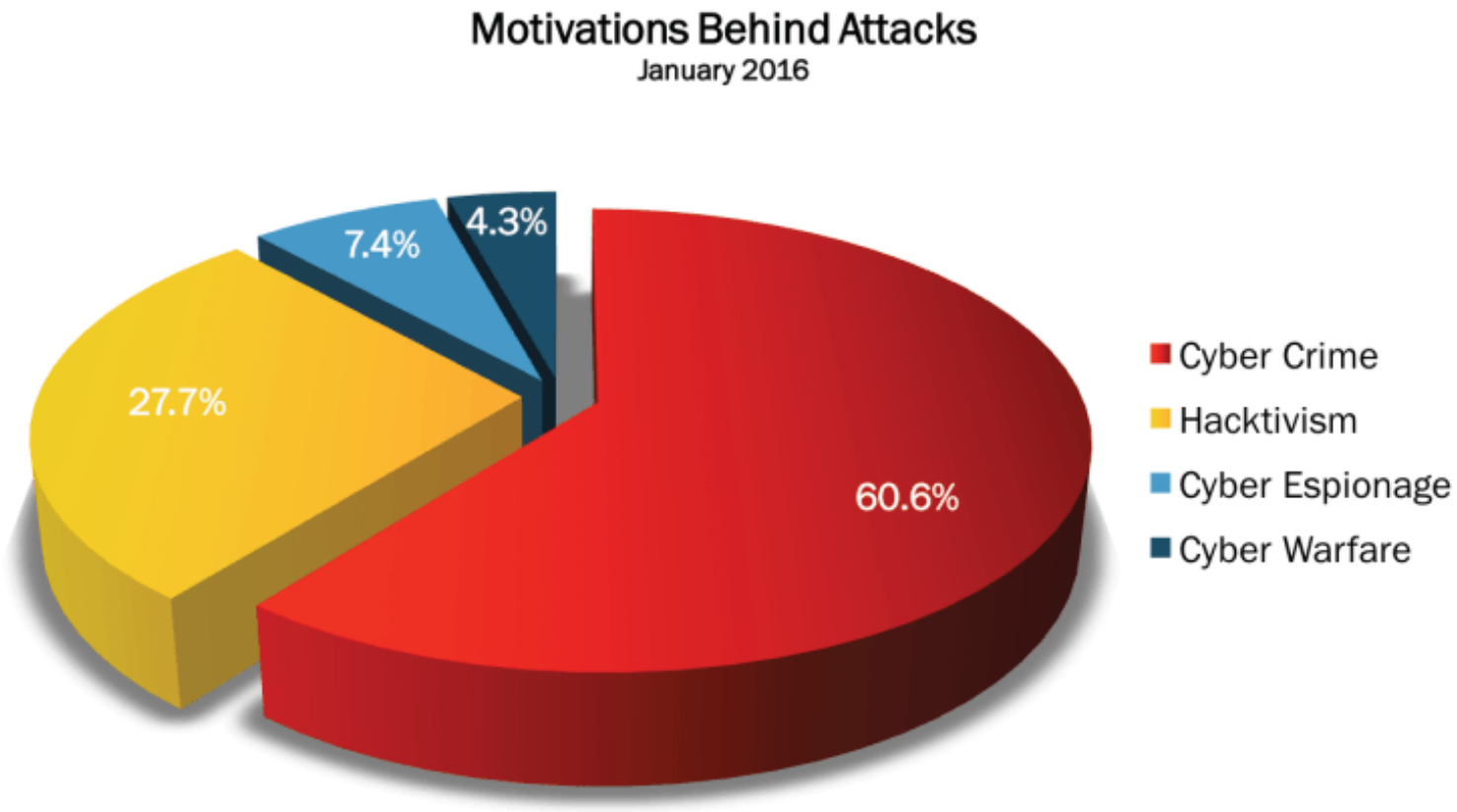
Cyber security is a category of solutions that partially address cyber risk. Cyber security is based on the principles of confidentiality, integrity and availability

Cyber risk is a category of business risks that have strategic, operational and regulatory implications. Cyber risk management assesses threats, vulnerabilities and its potential impact to the broader organization

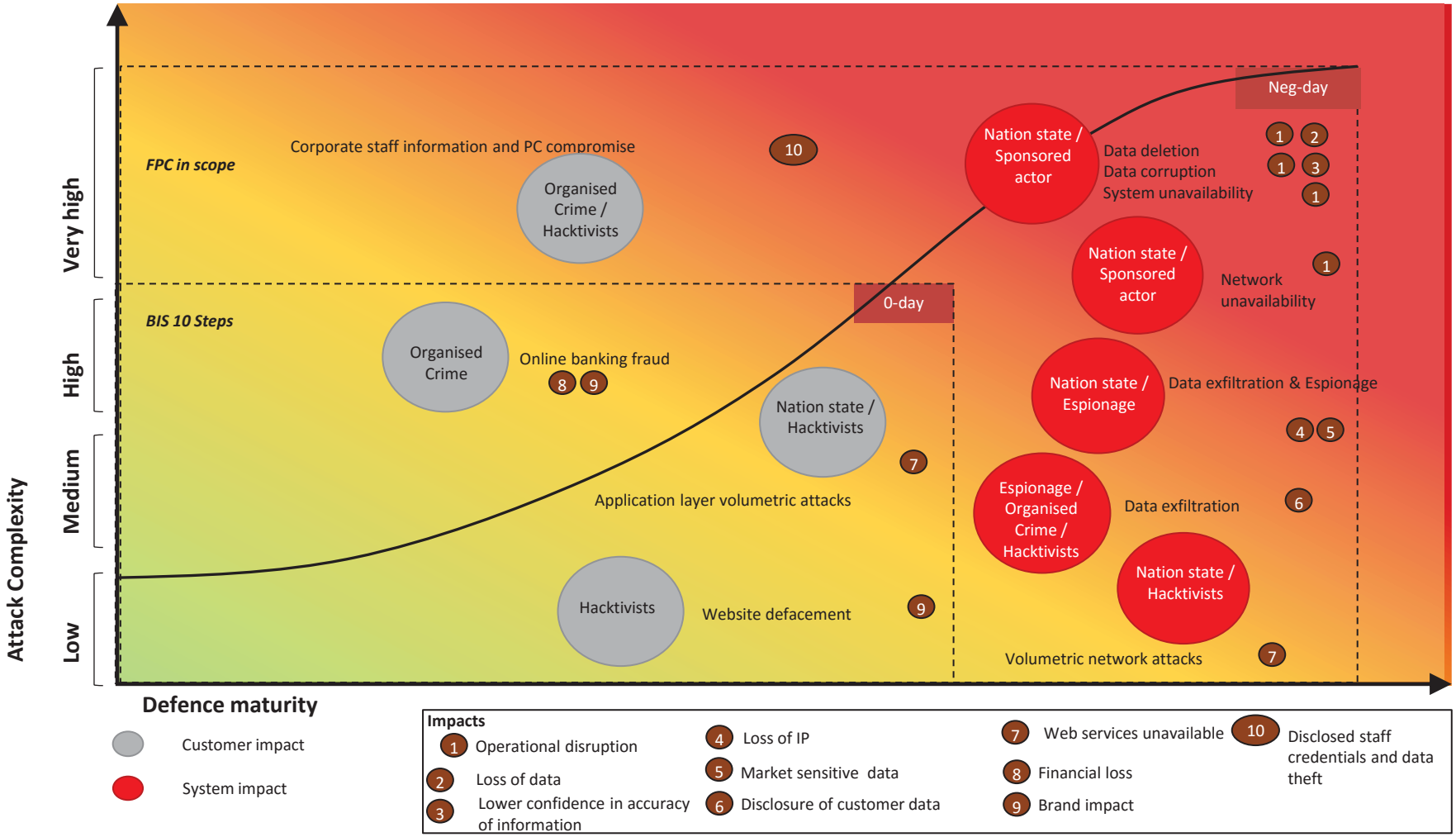
CYBER THREAT LANDSCAPE (DELOITTE)



MOTIVATIONS BEHIND ATTACKS

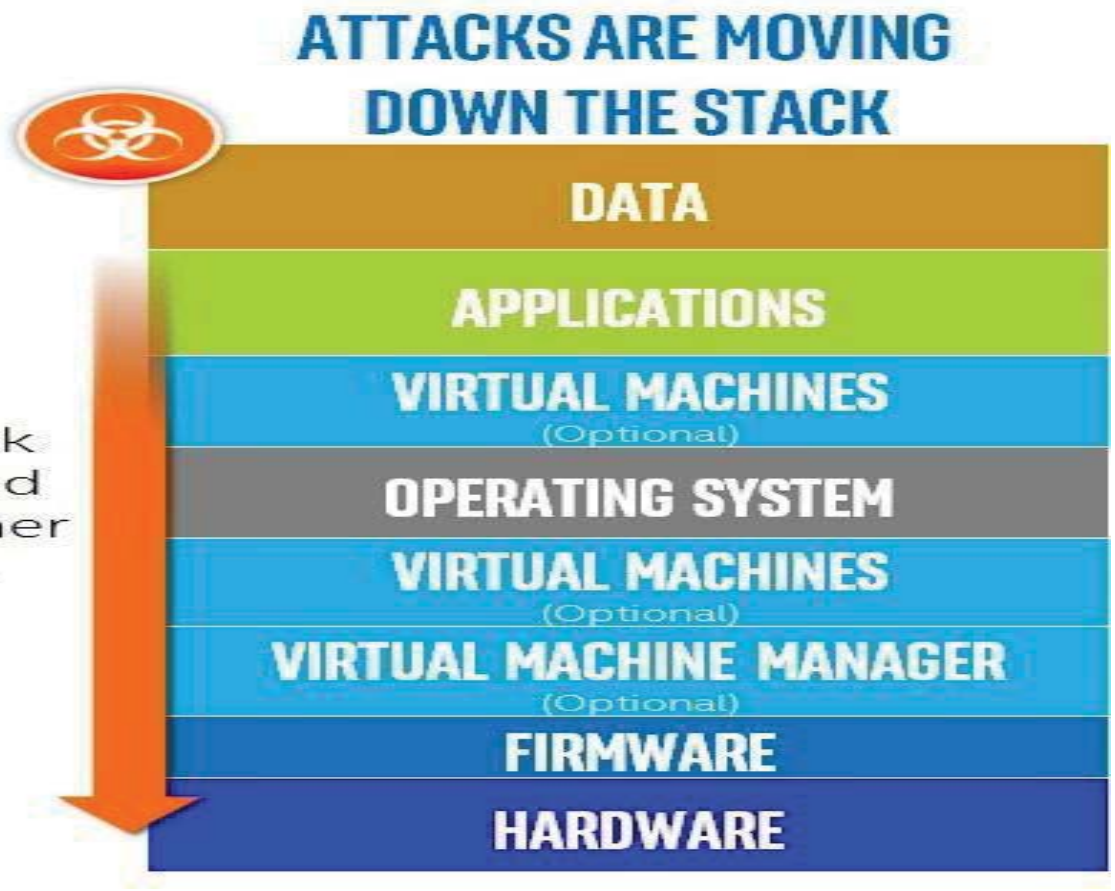


UNDERSTANDING THE THREAT

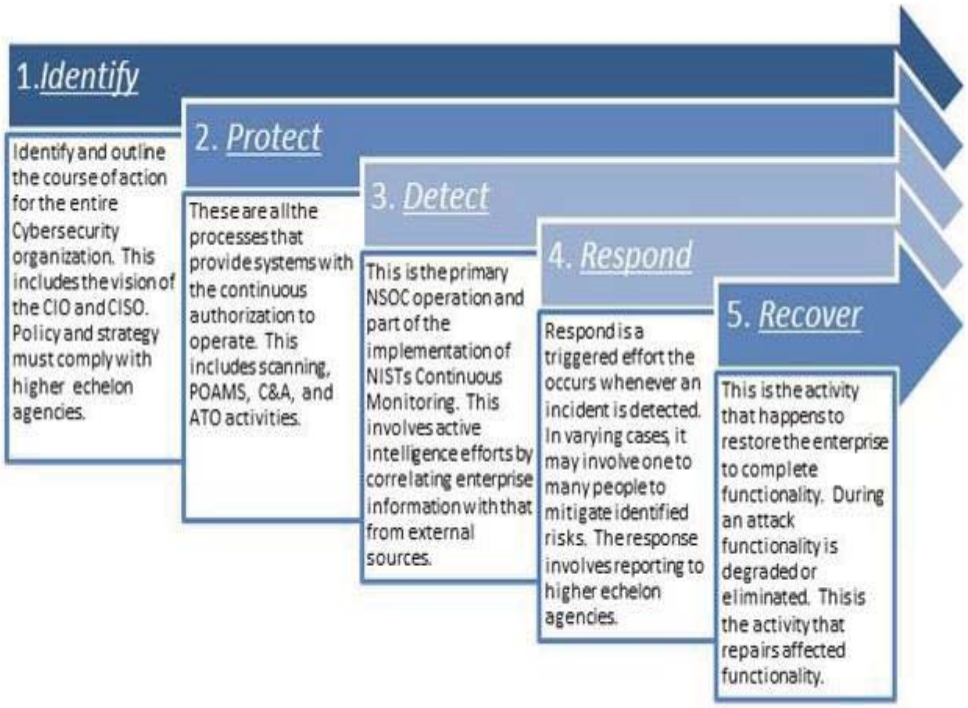


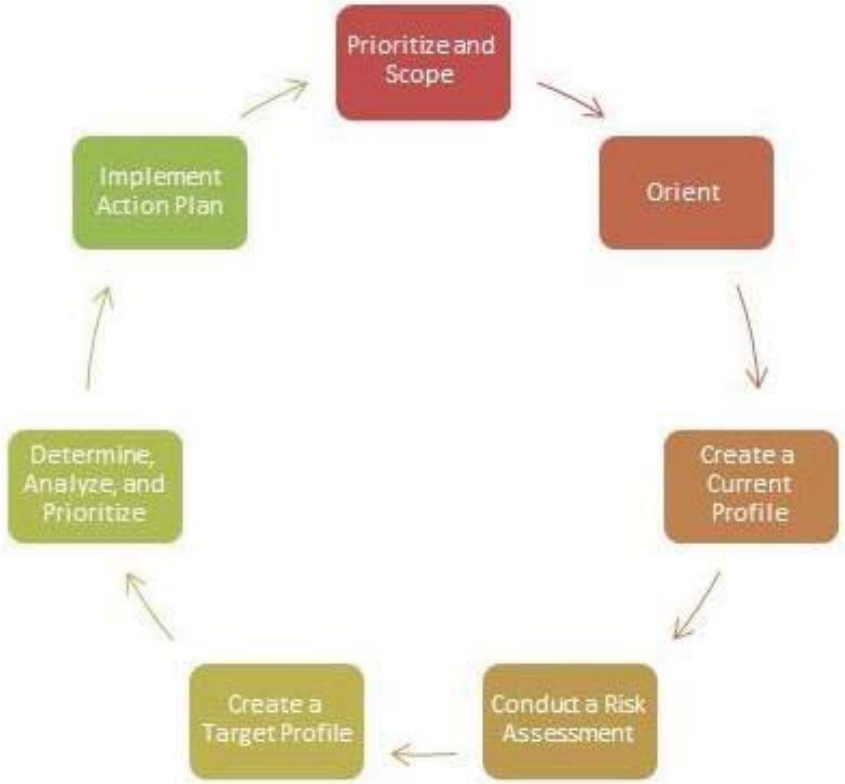
CYBERTHREATS SEEK ABSOLUTE CONTROL

Cyber threats seek greater control and opportunities further down the stack.



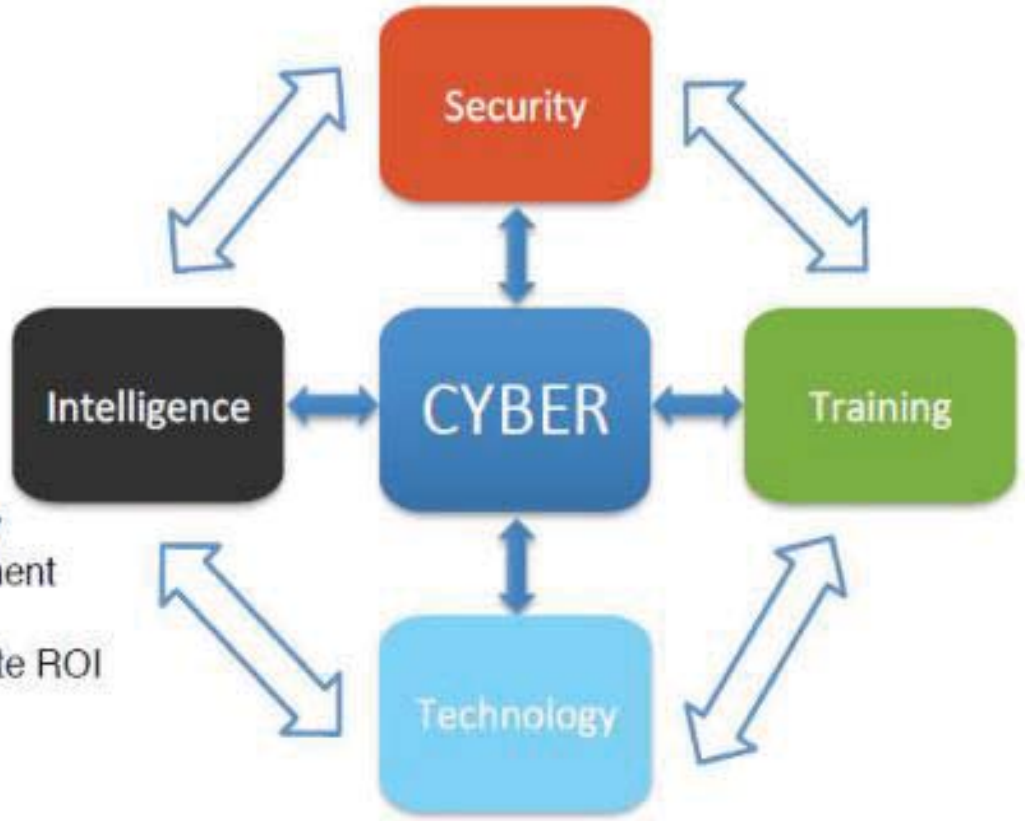
7 STEPS TO IMPROVE CYBERSECURITY OPERATIONS



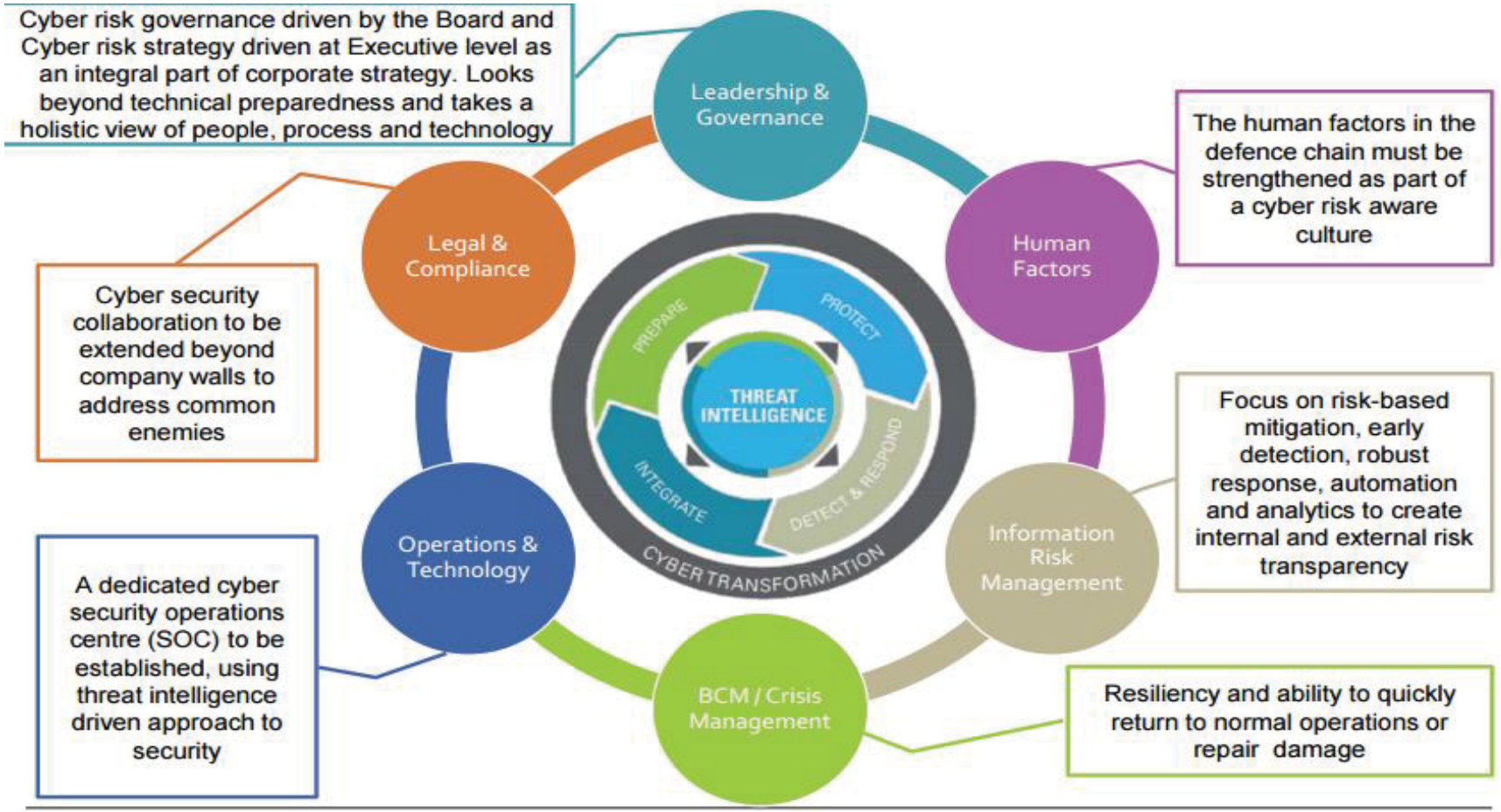


CYBER ECOSYSTEM- THE AWARENESS NEED

- ✓ Compliance and Assurance
- ✓ Privacy and Risk Management
- ✓ IT and Security Governance
- ✓ Continues Monitoring
- ✓ Threat Intelligence
- ✓ Critical Infrastructure Protection
- ✓ Increased speed of adoption
- ✓ Heightened awareness
- ✓ Identity, Credentialing, and Access Management
- ✓ Enhanced productivity and agility
- ✓ Incident Detection and Management
- ✓ Reduced training costs
- ✓ Turn-Key solutions with immediate ROI
- ✓ Group-up implementations
- ✓ Offensive & Defensive
- ✓ Cyber Exercises
- ✓ Cyber SITT as a Services



IMPLEMENTING A CYBER CORPORATE STRATEGY



CYBERINTELLINGE AND COMPLEX NETWORKS

Journal of Strategic Security

Volume 8
Number 3 *Volume 8, No. 3, Special Issue Fall 2015: Intelligence: Analysis, Tradecraft, Training, Education, and Practical Application*

Article 7

The Cyber Intelligence Challenge of Asyngnotic Networks

Edward M. Roche
Columbia Institute for Tele-Information, Columbia University, emr96@columbia.edu

Michael J. Blaine

John McCreary
Defense Intelligence Agency (ret.)

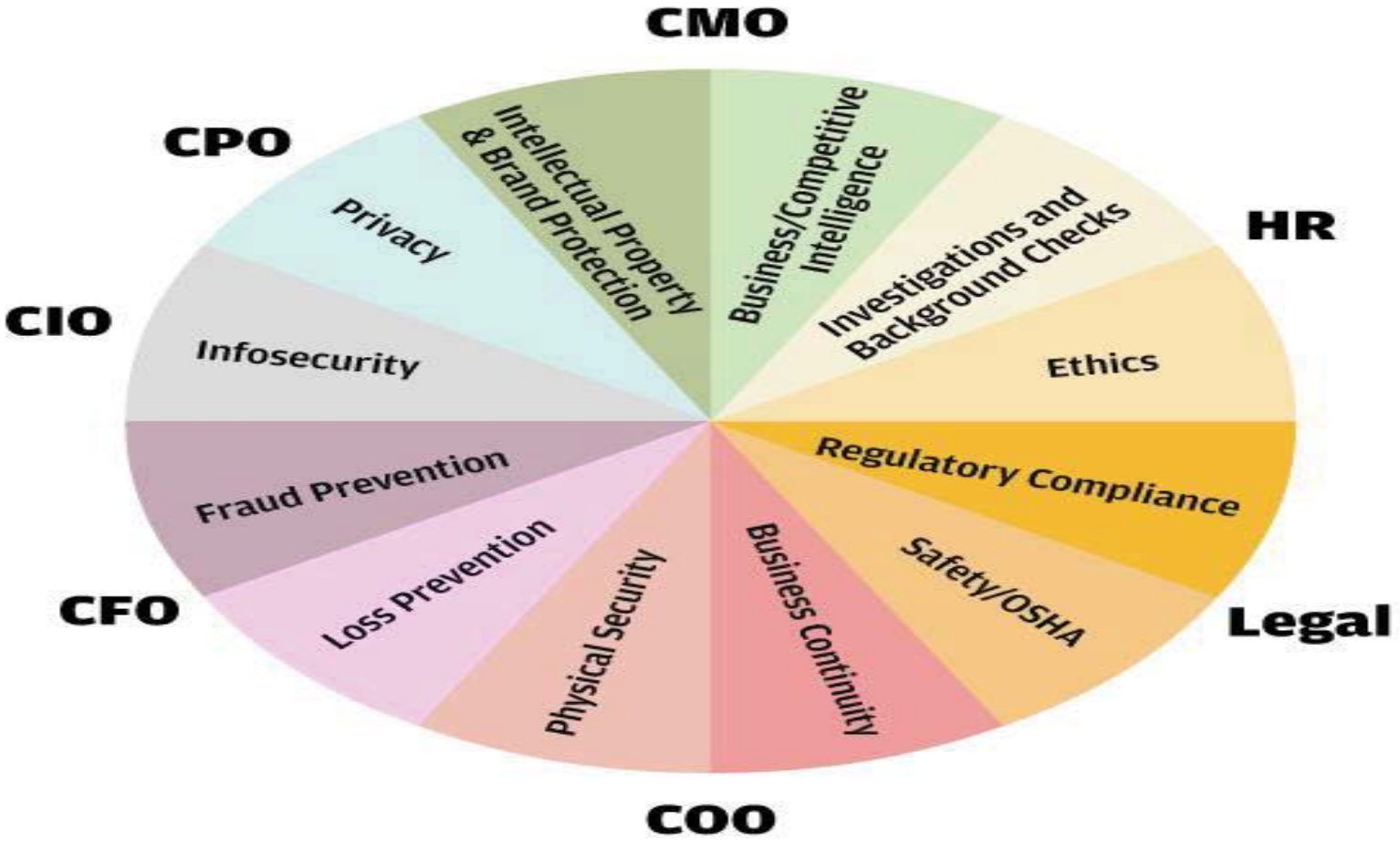
Abstract

The intelligence community is facing a new type of organization, one enabled by the world's information and communications infrastructure. These asyngnotic networks operate without leadership and are self-organizing in nature. They pose a threat to national security because they are difficult to detect in time for intelligence to provide adequate warning. Social network analysis and link analysis are important tools but can be supplemented by application of neuroscience principles to understand the forces that drive asyngnotic self-organization and triggering of terrorist events. Applying Living Systems Theory (LST) to a terrorist attack provides a useful framework to identify hidden asyngnotic networks. There is some antecedent work in propaganda analysis that may help uncover hidden asyngnotic networks, but computerized SIGINT methods face a number of challenges.

In order to examine this type of shadowy organization, we propose a simple framework that we call 'Asyngnosis'. The word is constructed from Greek: α- (not) + συνειδιτος- (conscious) + γνοσι- (knowledge, information); and describes the undirected emergence of knowledge and other interconnected pathways that form around a specific idea or activity. We would argue that an 'Asyngnodic' (+ δικτυο - grid or network) (an asyngnotic network) may describe many complex organizational activities, particularly decision-making and operations. Decisions and strategies may be modeled as not the outcome of a complex, structured set of discrete activities or processes, but instead as the product of continuous (non-discrete) flows of information, ideas and impressions ('memes')[15] along ever-changing communication pathways tying together individuals and organizations. Much like the pathways between neurons in the brain, these networks are characterized by their constant formation, strengthening, weakening, and disappearance based on use and need, yet as these connections and disconnections take place, the organization itself constantly changes.[16]

CYBERINTELLIGENCE

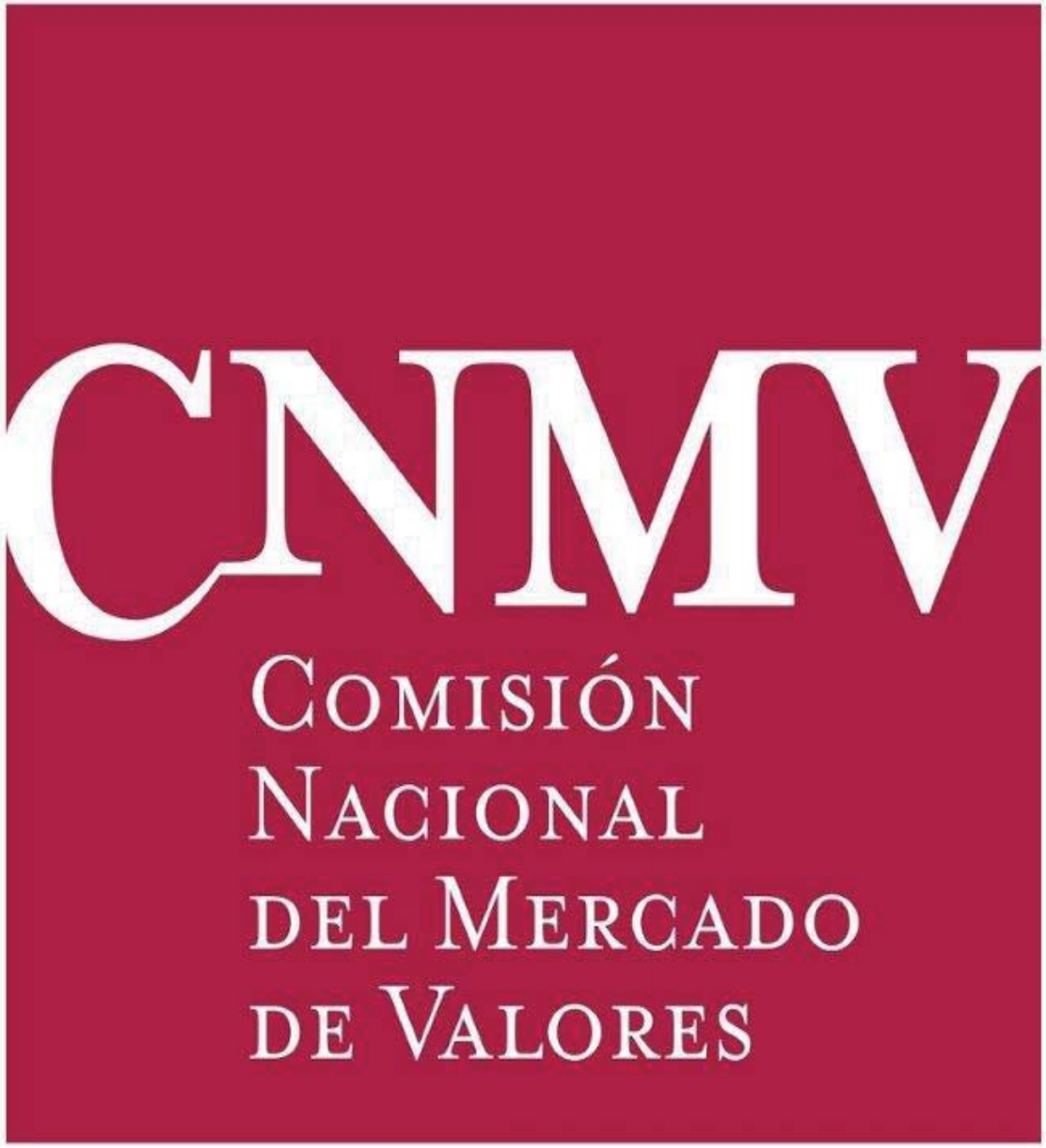
CHIEF SECURITY OFFICER SKILLS: NEW ROLE



THE IMPORTANCE TO ADOPT PREVENTION MEASURES

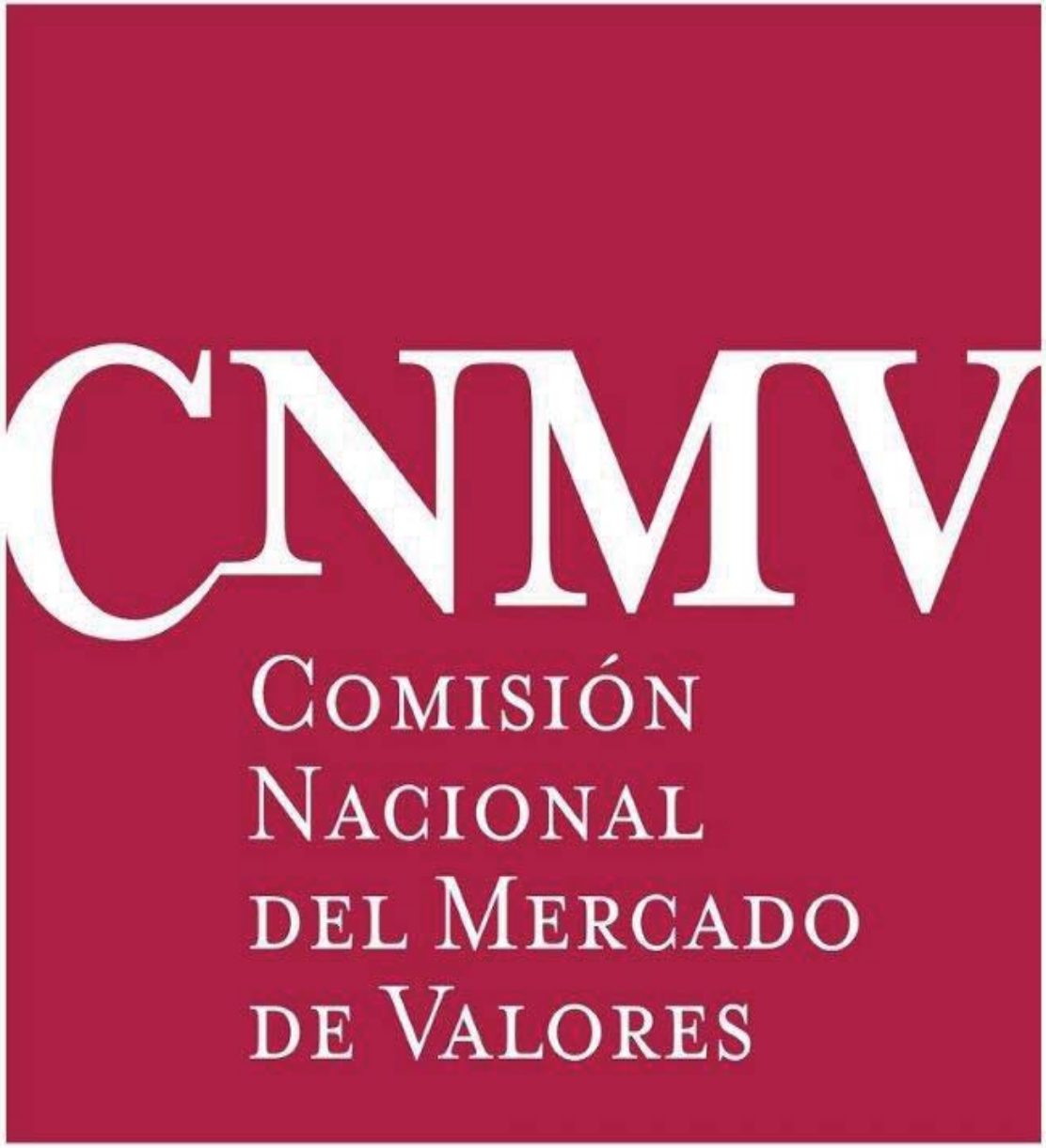
The evolving nature of cyber threats increases the need for sound management practices and a strong, professional risk culture in financial institutions which can react to new threats and deliver appropriate levels of employee awareness about new risks. Moreover, supervisors, institutions and policymakers alike should cooperate to seek further remedies to address cyber and IT risks. They should also consider the use of market-wide exercises involving the industry and public authorities to improve coordination in the face of large-scale cyber-attack. Given the profits that organised criminals can obtain by means of fraud, industrial espionage or sabotage, this trend will in all likelihood continue to gather pace.


ecix
next
International
Business School
WALHALLA
WHEN DATA IS CRITICAL


CNMV
Comisión
Nacional
del Mercado
de Valores

VISION DE LOS REGULADORES SOBRE CIBER SEGURIDAD. INFORME DE IOSCO

Tajinder Singh
Vicesecretario General de IOSCO


CNMV
Comisión
Nacional
del Mercado
de Valores

Clausura

Convergencia supervisora en el ámbito de los mercados de valores

Lourdes Centeno
Vicepresidenta de la CNMV