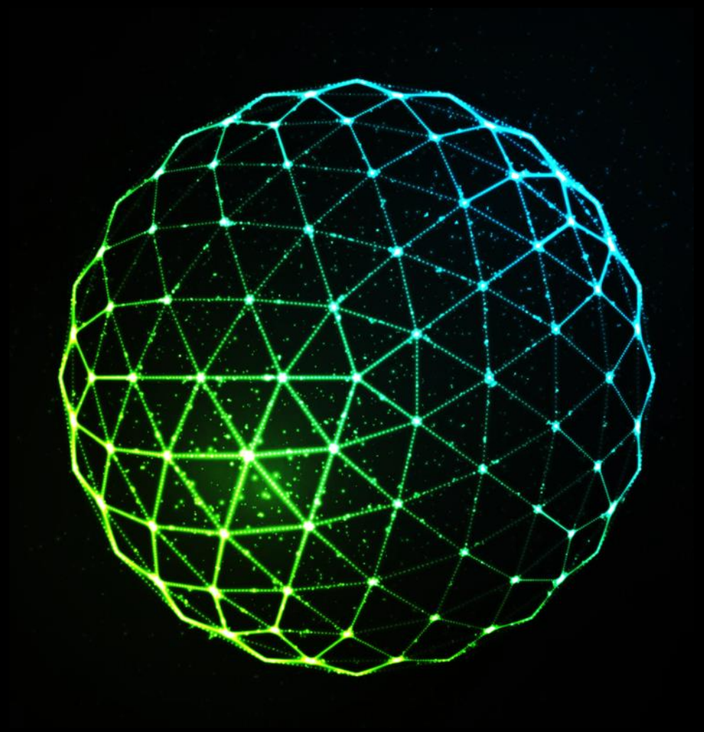
Deloitte.

Cyber Singularity

Business Modernization comes to Cyber

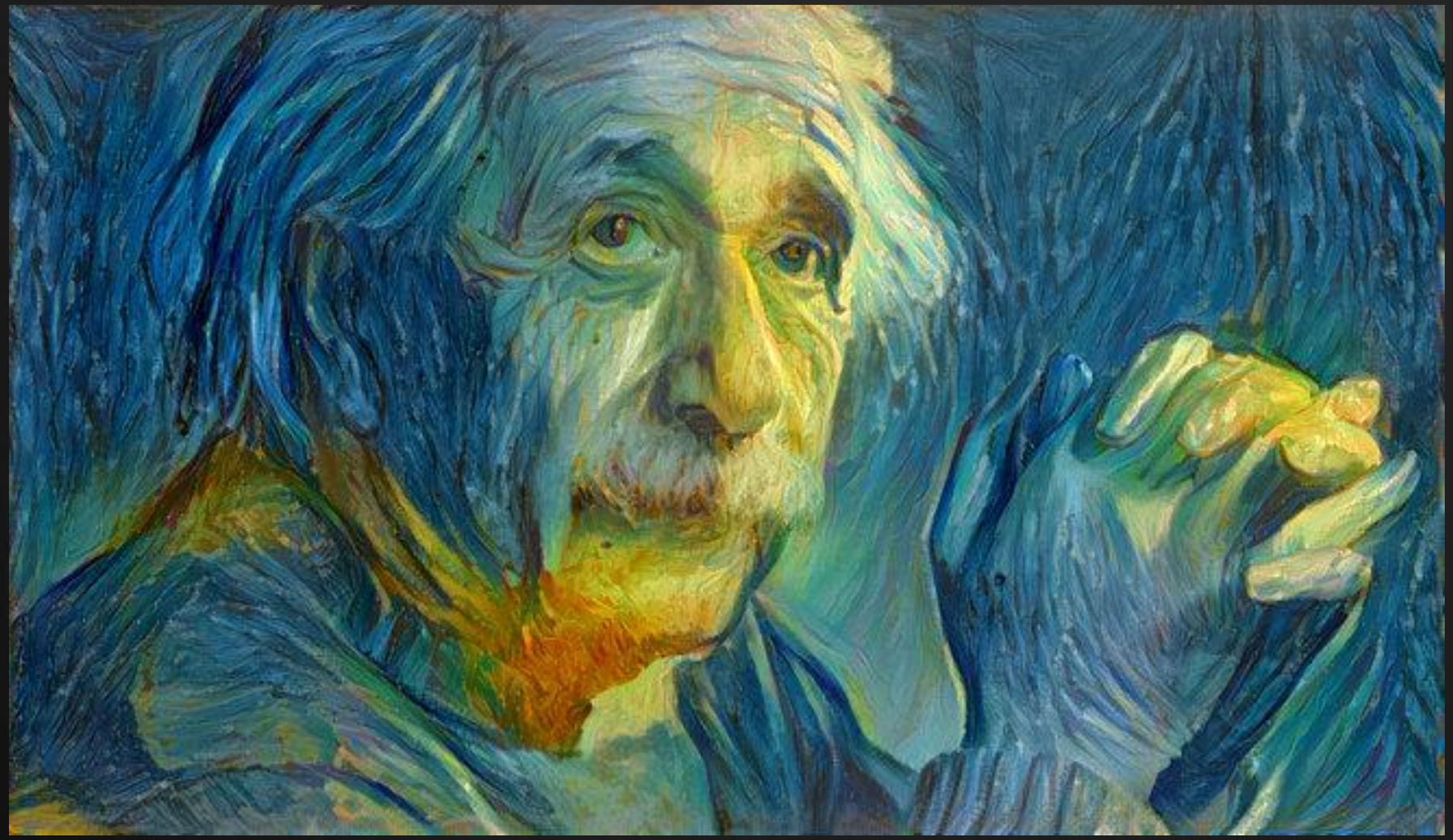
IEEE UAE CYBER INTELLIGENCE SUMMIT

October, 2018



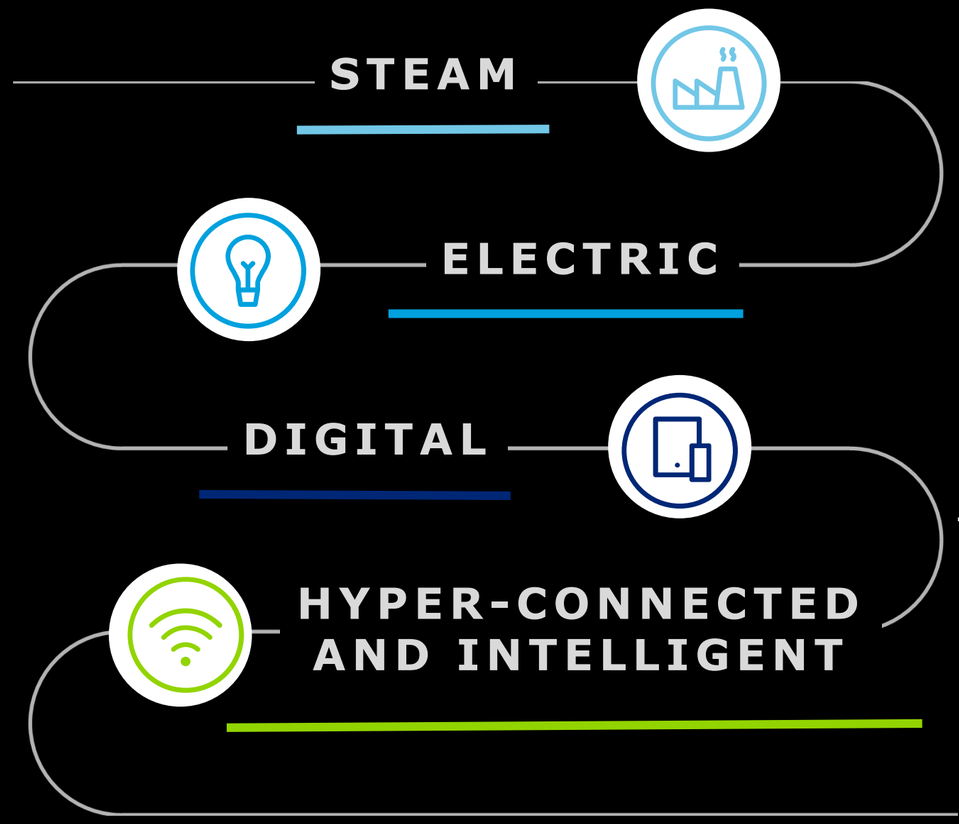
Center for
STRATEGIC CYBER INNOVATION
GLOBAL

More to come



2018 Deloitte Cyber Risk Services

The changing business and cyber risk landscape



1990 - 2002

Era of Infrastructure

2002 - 2010

Era of Compliance

2011 - 2016

Era of Risk

2016+

Era of Ubiquity

2018 Deloitte Cyber Risk Services

Cyber driving Business Modernization

Cyber is rapidly becoming a business imperative

Digital is becoming an essential business disruptor

Organizations are quickly coming to the realization that Cyber provides a platform to engage with their customers in an agile, cost effective manner. Expanding products and services is becoming an essential transport for profitability and business growth.

Digital transformation is linked to National Prosperity

Organizations are starting to use and promote the protection of their customers, partners and employees as a competitive differentiator. As cyber issues continue to be associated with geo-political events we anticipate this theme to accelerate in the next decade.

Rate of Change

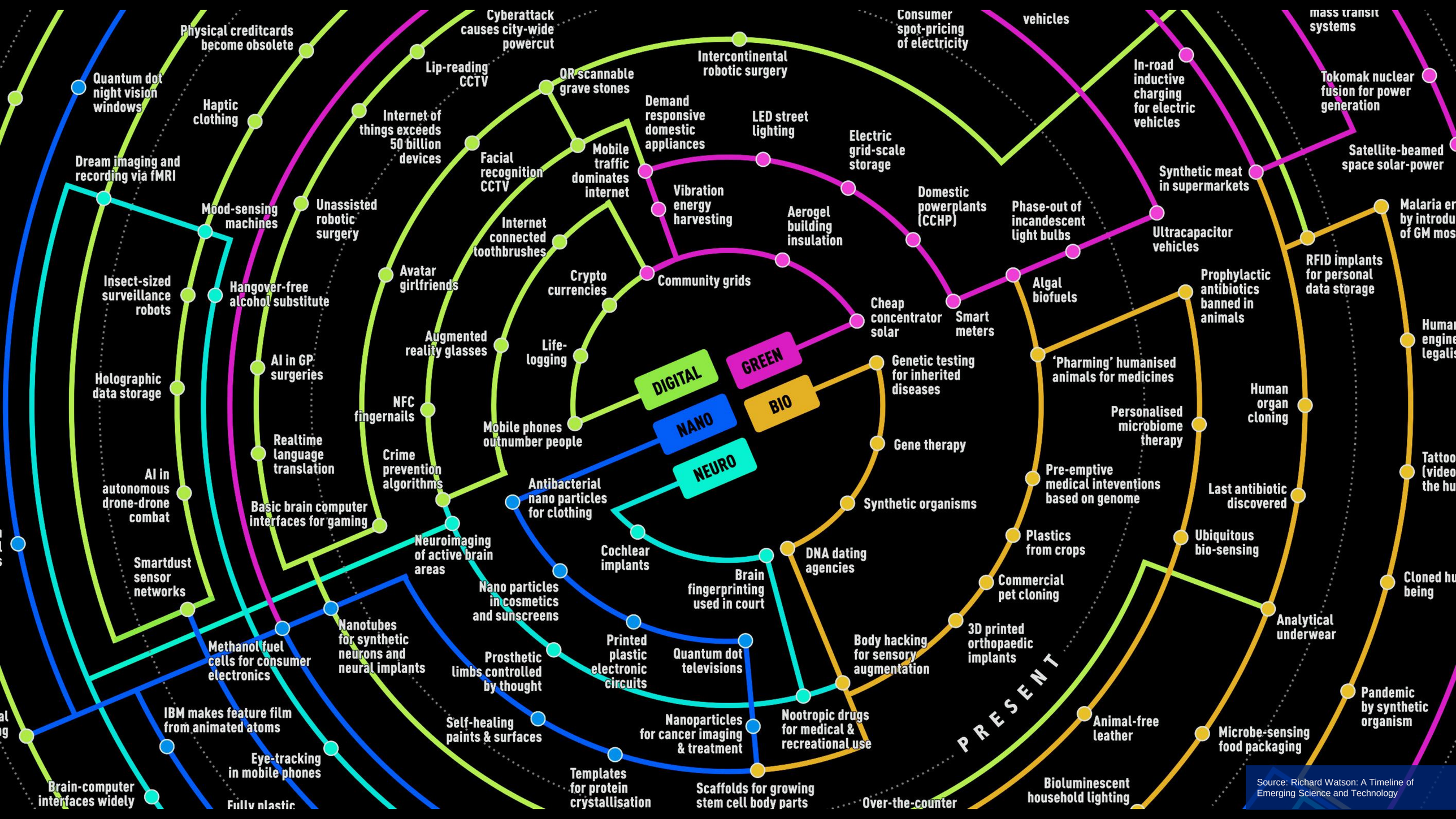
Innovation, digital transformation and business modernization is essential for Canada's standing, globally. In order to serve our country, citizens and community we need to need to be in the forefront of innovation and transformation of our economy.

Cyber increasingly being used for Strategic Purposes

Cyber is increasingly being used for strategic interests, as an asymmetric lever. The ability to "move markets", national priorities and trade is accelerating the need for sound cyber resilience.

Financial Gain through Cyber is accelerating acceptance

Due to the financial, geo-political and nation benefits, actors have the motivation to invest in increasingly sophisticated methods. Most of our clients do not have the (global) scale, consistency in expertise and focus, driving the need for expertise that can be afforded by our firm).



Source: Richard Watson: A Timeline of Emerging Science and Technology

D - Trust

D1 - Data Sovereignty

Evolving regulatory context around data privacy creates new challenges and "road bumps" for adapting digital transformation.

D2 – Channel, Third Party and Partner Trust

Higher emphasis on building "rings of trust" between suppliers, vendors and partners, extends risk management.

A - Disruption

A1 - Global Competition

Atypical competitors ranging from Fintech, globalization and typical cyber companies moving into alternative service offering.

A2 – Alternative Business Models

Non-traditional players are disrupting age old business models.

A3 - Innovation Acceleration Pressures

Stakeholders, customers and industry forcing rapid innovation.

C - Technology

C1 – Business appetite

IT Innovation and the use of "Exponential Growth" drives higher attack surface.

C2 – Customer demographics

"Digitalization" of the generation entering into the working population driving increased adoption of digital platforms, innovation and progressive solutions.

C3 - Automation and AI

Entering the "era" of large scale use of automation driving a digital industrialization of work force.

C4 - Open Economies

Geo-Political trending towards open standards, wealth democratization and open money.

B - Asymmetrical Capability

B1 - Cyber Advancement

Adversaries and offensive method fast approaching Cyber Singularity

B2 - Adversary Investment

"Rinse and repeat" model drives larger attack surface and significant Reward/Risk equation.

B3 – Increased Attack Surface

Adversaries have an ever growing attack surface to exploit.

B4 - Extended Enterprise

Due to the "extended" enterprise and other exponential methods, attack surface is growing.

2018 Deloitte Cyber Risk Services

Deloitte.

CYBER SECURITY DRIVEN BY GLOBAL MEGA-TRENDS

Global undercurrents help shape commerce, trade and business behavior of our clients. Our goal is to get ahead of the curve to help define new markets, service opportunities and revenue streams.

GLOBAL MEGA TRENDS

Global mega trends create the backdrop for business, trade and the basis to drive industry. Global trends are often re-enforced through regulation, customer behavior and other related factors.

COMMERCE, TRADE AND BUSINESS

To ensure continued commercial relevance, growth and strategic viability, organizations invest and continue to innovate around mega trends.

CYBER THREATS LANDSCAPE

Global Mega-Trends lead to changes in cyber threat landscape.

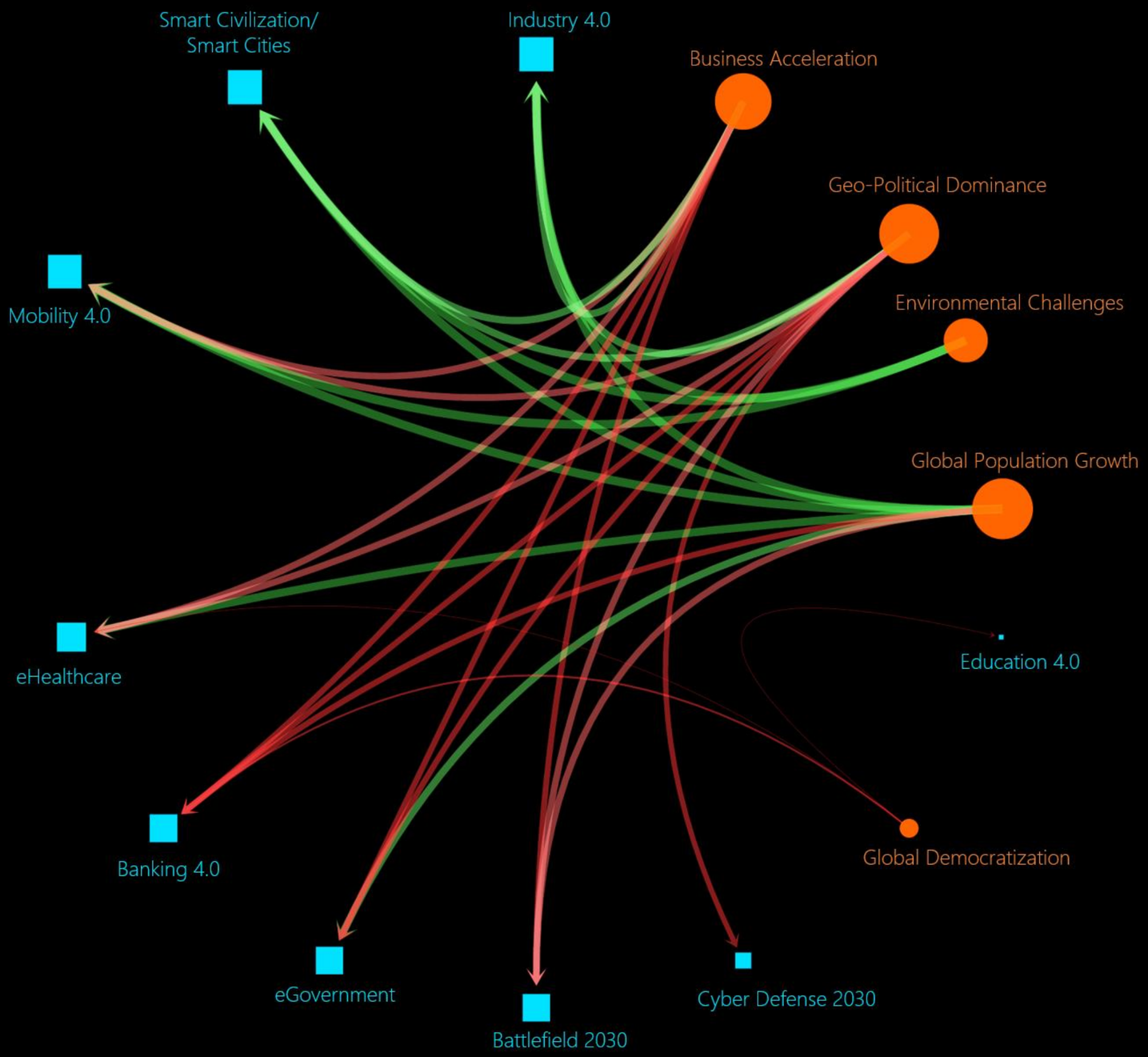
CYBER DEFENSE

Cyber defenses allow organizations to accelerate their strategic goals.

Global Mega Trends – Cyber Perspective Outcome Innovation Domains

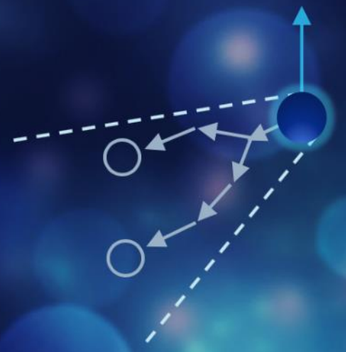
Cyber Innovation is derived from customer, industry and government innovation. Similarly commerce is driven through Global Mega Trends.

The graphic to the right illustrates how a sample of **global trends** will result in the acceleration of trends that can be capitalized through Cyber Perspective Outcome Innovation.



ACTOR TRADE CRAFT EVOLUTION

ACTOR TRADECRAFT
CATEGORY 1 - LINEAR



Traditional actor exploit techniques utilizing linear threat methods. This includes brute force, available exploit kits, singular attack methods. Threats typically associated with this tradecraft includes (but not limited to):

- DDoS
- Disruption
- Brute Force
- Application Exploits
- XSS and Buffer Overflow

ACTOR TRADECRAFT
CATEGORY 2 - EVASION

Advanced TTP based actor tradecraft broken down into a primary and evasion objective. This is typically used for high value targets, such as:

- Customer takeover
- Surveillance
- Strategic data gathering (adversary or state actor)

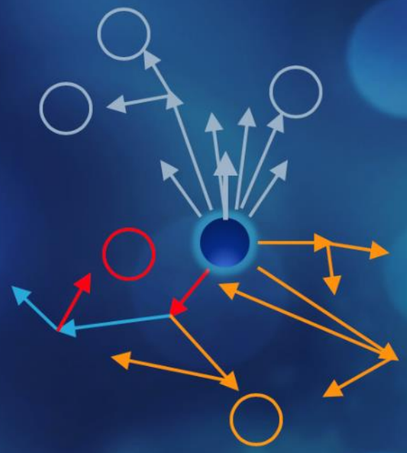
ACTOR TRADECRAFT
CATEGORY 3 - DIRECTIONAL CAMPAIGN

Campaign based directional kill chain. This is typically used by a military trained actor that breaks down the overall mission into specific campaigns. This actor tends to be patient and measured.

The approach used by red/purple teams on this approach includes (but not limited to):

- Multi-threaded mission
- Covert and “smoke screen” methods

ACTOR TRADECRAFT
CATEGORY 4 - REFRACTED CAMPAIGN



An enhanced version of kill chain. This tradecraft is associated with an adaptive (focus on machine learning) actor which utilizes a “refracted” exploit techniques, which federates entry points, access paths and other measures.

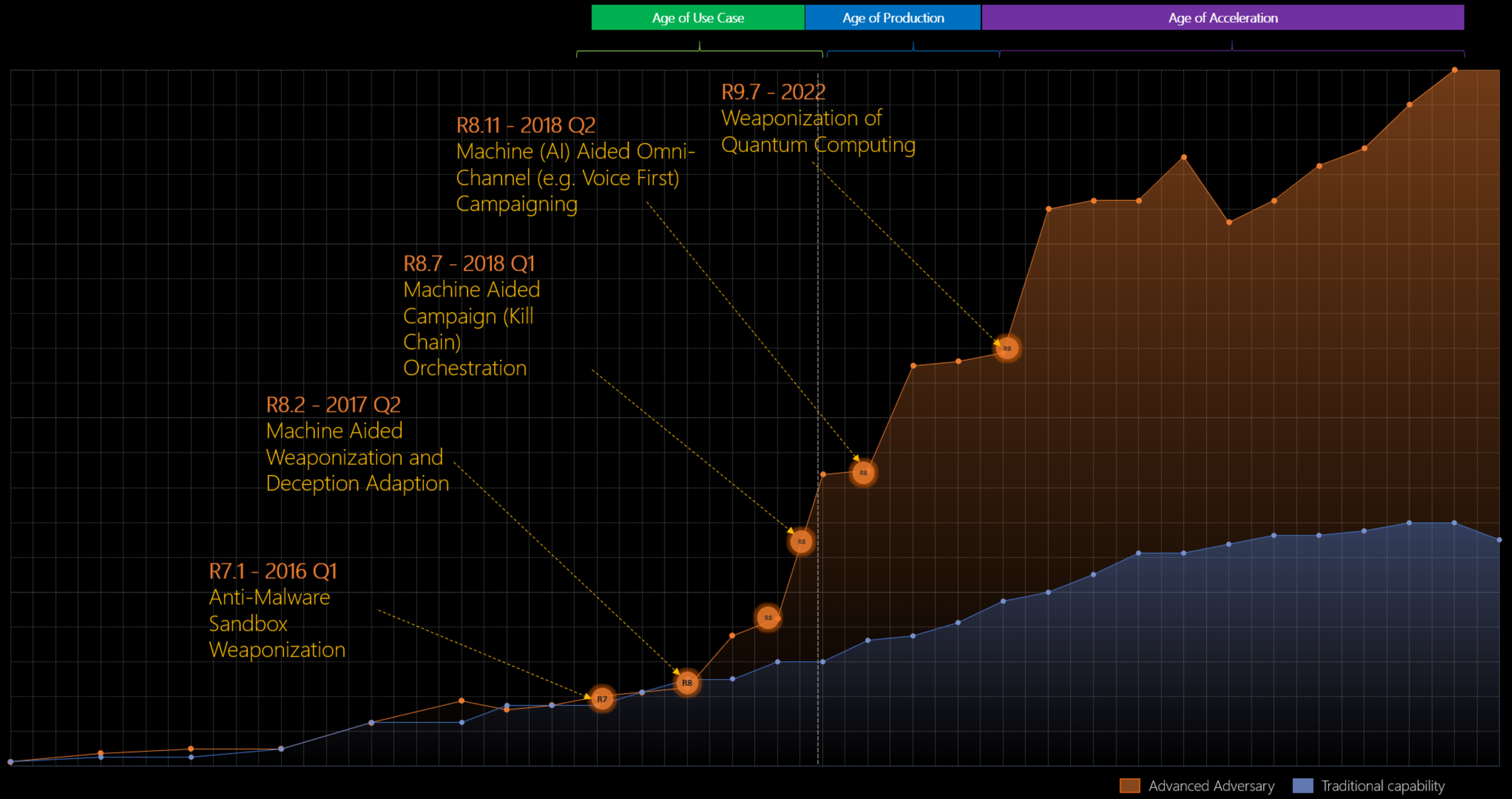
The approach used by red/purple teams on this approach includes:

- Sophisticated financial crime/syndicate
- Use of data for asymmetric capability
- Machine learnt adaptive kill chain

Conventional TTP | Covert/Diversionary TTP | Advanced TTP | Human Predation

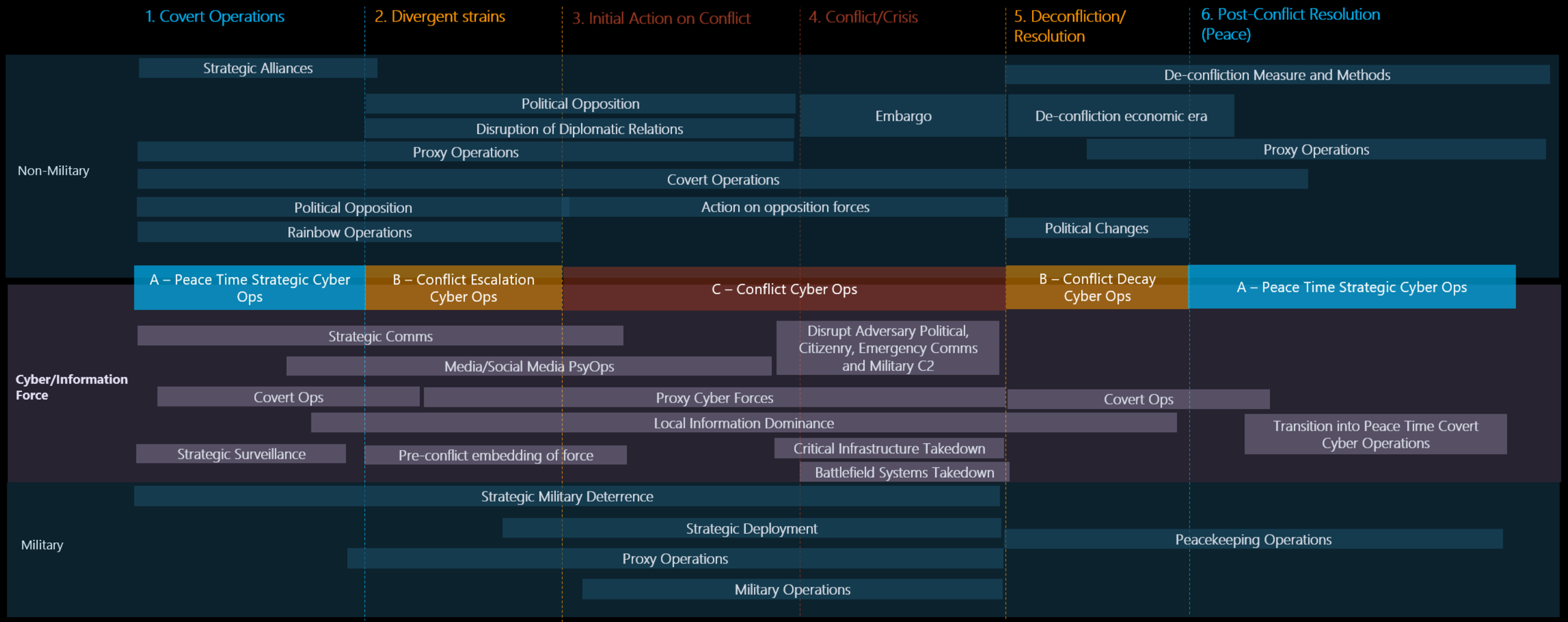
2017 Deloitte Cyber Risk Services

Coming of Cyber Singularity - Weaponization of Cyber Artificial Intelligence



Deloitte. Cyber Risk Services | Threat Lifecycle Management

Case Study 2 – Cyber as a Geo-Political Lever (contd.)



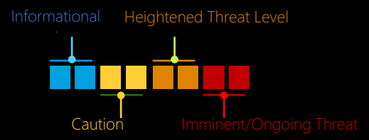
2018 Deloitte Cyber Risk Services

A – Peace Time Cyber Ops

- Financial Services and Exchange
- Insurance
- Transportation
- Oil and Gas
- Power Distribution, Generation and Utility
- Retail
- Telecommunication/Technology
- Media
- Manufacturing
- Education
- Public Sector
- Defense
- Healthcare

B – Conflict Escalation

- Financial Services and Exchange
- Insurance
- Transportation
- Oil and Gas
- Power Distribution, Generation and Utility
- Retail
- Telecommunication/Technology
- Media
- Manufacturing
- Education
- Public Sector
- Defense
- Healthcare



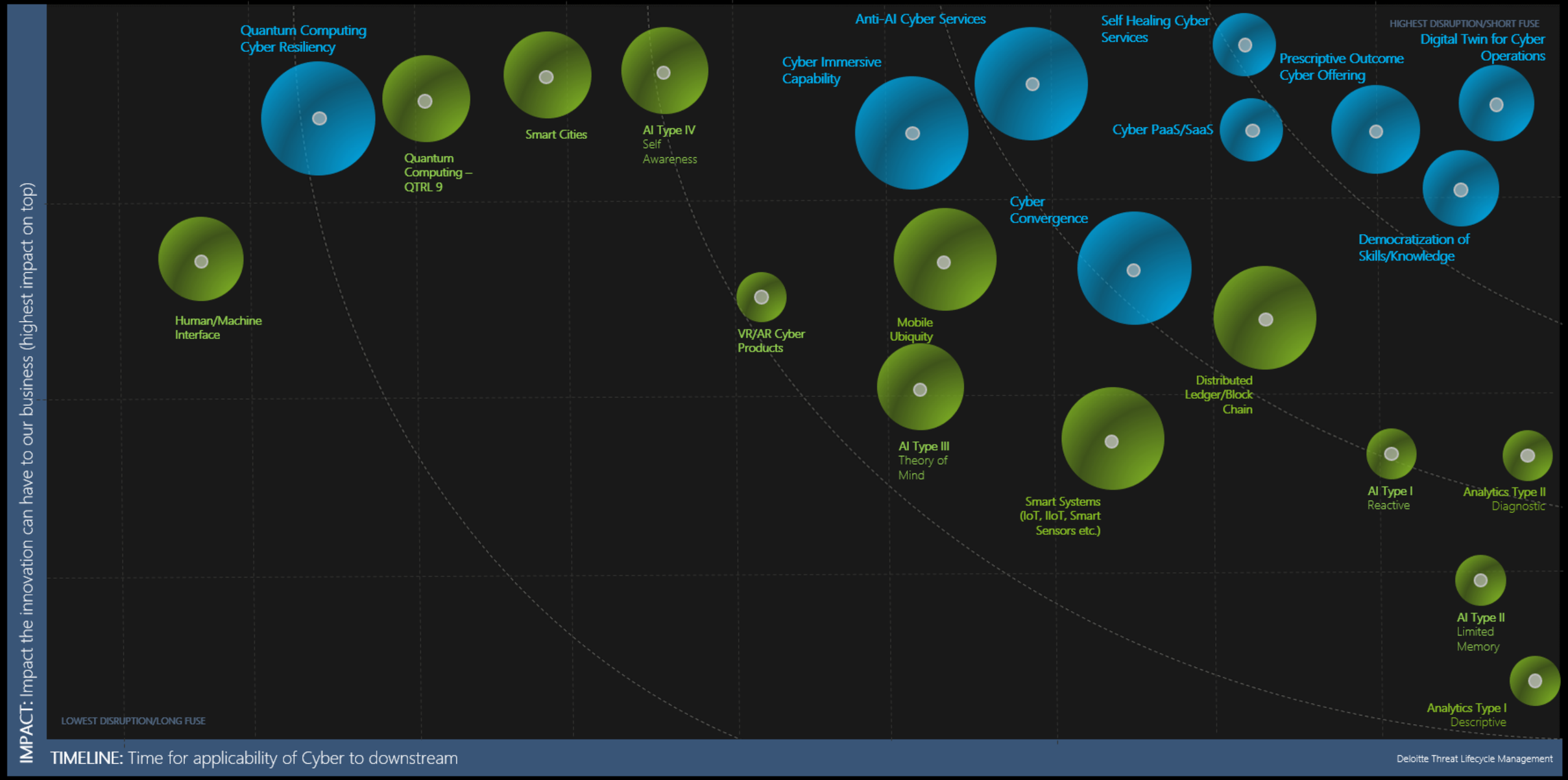
2018 Deloitte Cyber Risk Services

Examples of pre-conflict operations

- Psychological Operations (PhysOps): Using disinformation, surveillance and disclosure to influence democratic processes or cause institutional chaos (to deter governments from focusing on geo-political initiatives);
- Oil and Gas: Conducting strategic data analytics against surveillance telemetry data (e.g. oil production value) to understand concentration of energy supply chain that can be disrupted where required);
- Power Generation and Distribution: Similar to the oil and gas example, conducting strategic data analytics on power distribution to determine concentration of industry and critical infrastructure that can be disruptive in the event of escalated campaigns;
- Logistics: Conducting surveillance on the movement of (e.g. food) supplies as a method of determining troop movement; or
- Connected Systems: Using bio-data (e.g. fitness data) to assess concentration of military personal or movement of troops.

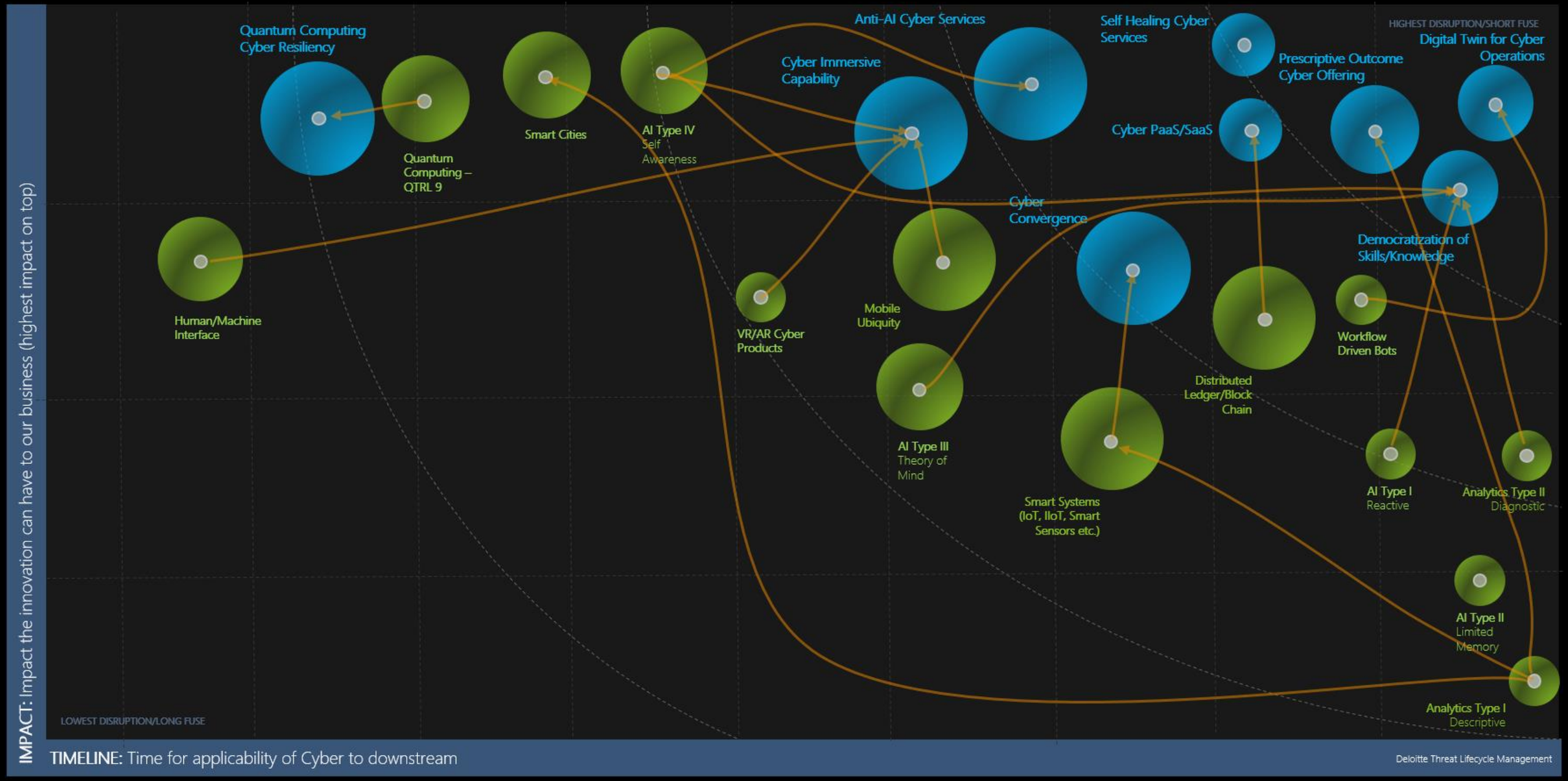
2018 Deloitte Cyber Risk Services

How Business Modernization is driving Cyber



2018 Deloitte Cyber Risk Services

How Business Modernization is driving Cyber



CYBER POWERING COMMERCIAL INNOVATION

HUMAN IMAGINATION AND APPLICATION OF INNOVATION IS LIMITLESS

The rate of global disruption, powered by cyber is virtually limitless. Rate is constrained by a number of factors. Some of the key aspects include.

01

RESOURCES

The allocation of resources, innovators, funding and capability to assign to transformation and cyber enabled innovation.

02

COMPREHENSION

The ability to comprehend the rate of change and how it applies to their industry, customer and stakeholders.

03

WILLINGNESS

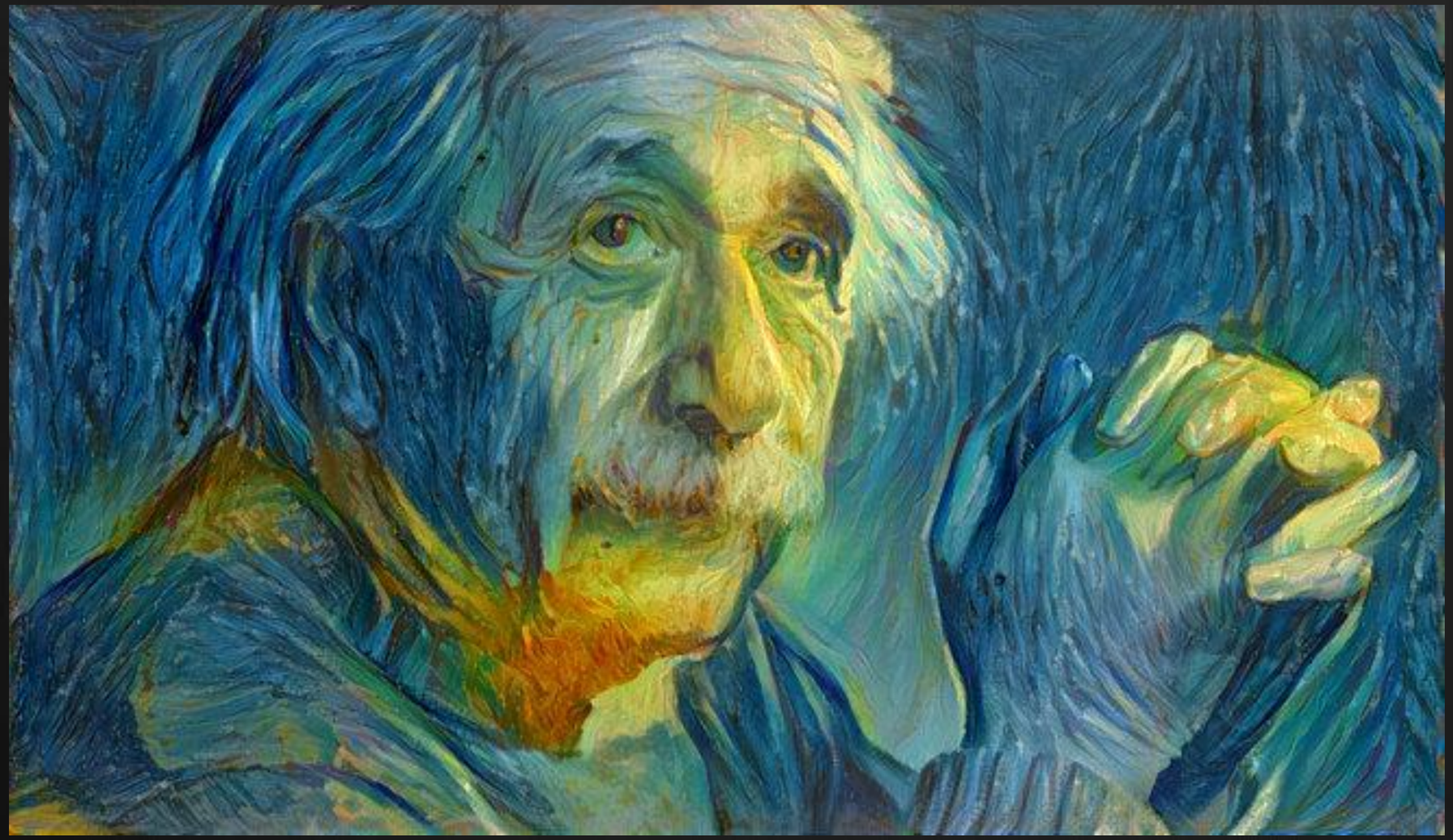
The willingness to embrace change and challenging institutional orthodoxy.

04

CAPABILITY

The availability of enabling capability to enable innovation.

More to come



2018 Deloitte Cyber Risk Services