Le (sempre più) numerose facce del rischio cibernetico all'interno della vorticosa trasformazione digitale

Roberto Baldoni, già primo Direttore Generale della Agenzia per la Cybersicurezza Nazionale, vice Direttore Generale del Dipartimento Informazioni per la Sicurezza e da vent'anni Professore Ordinario di Cybersecurity presso La Sapienza di Roma

OLTRE L'ORIZZONTE: sfide attuali e futuri possibili per le Piccole Medie Banche italiane
San Marino 24 Novembre 2023

Un mosaico di complessità

CLOUD BLOCKCHAIN NANOTECH

ROBOTICS

Trasformazione Digitale

SENSORS

MICROCHIP

QUANTUM COMPUTERS

AI IoT

Globalizzazione

Supply Chain

Interdipendenza

Dipendenza

Resilienza

Un mosaico di complessità

CLOUD BLOCKCHAIN NANOTECH

ROBOTICS

MICROCHIP

Trasformazione Digitale

SENSORS

QUANTUM COMPUTERS

AI IoT

Geopolitica

Sicurezza nazionale

Stabilità Globale

US-China tug-of-war

Egemonia tecnologica

Globalizzazione

Supply Chain

Interdipendenza

Dipendenza

Resilienza

«You may not be interested in geopolitics, but geopolitics is interested in you»

Ken McCallum Chief of UK Intelligence

«Puoi non essere interessato alla geopolitica, ma la geopolitica è interessata a te»

OLTRE L'ORIZZONTE San Marino 24 Novembre 2023

Infrastrutture critiche

Tecnologie all'avanguardia

Cittadini

Rischio Cibernetico

«Fully secure systems don't exist today and they won't exist in the future»

Adi Shamir, the «S» of the RSA public key cryptosystem

«Sistemi sicuri non esistono oggi e non esisteranno in futuro»

Attacchi cyber

Rischi dalle catene di approvvigionamento

Disinformazione& ingegneria sociale

Intelligenza artificiale & Computer quantistici

Mancanza di competenze

Rischio Cibernetico


Ministero dell'Interno

MF

17-NOV-2023
Estratto da pag. 1-2

ESCLUSIVO I RISULTATI DELLE ISPEZIONI IN 22 GRANDI ISTITUTI EUROPEI

Cyber-crepe nelle banche

Allarme della Vigilanza: le lacune scoperte sono più gravi e diffuse del previsto
Bce molto preoccupata. Manager strigliati: contromisure immediate e concrete

Ninfole e Savojardo alle pagine 2 e 3

BCE I RISULTATI DELLE ISPEZIONI CONDOTTE IN 22 GRANDI ISTITUTI IN 11 PAESI EUROPEI

Banche, allarme sui rischi cyber

Per la Vigilanza le lacune sono risultate più gravi e diffuse del previsto. Francoforte invita anche a rafforzare la presenza in Ue dopo Brexit. Lagarde: attenzione agli npl

- Attacchi cyber
- Rischi dalle catene di approvvigionamento
- Disinformazione& ingegneria sociale
- Intelligenza artificiale
- Mancanza di competenze

Compliance

Europe
- EU Network Information Infrastructures Directive (NIS II)
- EU Digital Operator Resilience Act (DORA)
- EBA ICT guidelines
- EBA governance guidelines
- EU General Data Privacy Regulation
- European Central Bank framework and test

Italy
- BoI retail payment system regulation
- BoI cybersecurity guidance
- BoI&Consob regulations of trading venues, banks , and investment firms
- ACN National Security Perimeter Law for Cyber

Industry
- PCI/DDS
- ISO IET 27001
- SWIFT CSP

Attacchi cyber

Rischi dalle catene di approvvigionamento

Disinformazione& ingegneria sociale

Intelligenza artificiale

Mancanza di competenze

Rischio Cibernetico

«Può la compliance salvarmi dalla minaccia cyber?»

«la risposta è no! La compliance aumenta la resilienza del sistema»

Attacchi cyber

Rischi dalle catene di approvvigionamento

Disinformazione& ingegneria sociale

Intelligenza artificiale

Mancanza di competenze

Rischio Cibernetico

State-sponsored attacks
Cybercriminals
Hactivists

GEOPOLITICS
TECHNOLOGY

Attacchi cyber

Supply chain interruption
Integrity of licensed products
Tampering managed services

GEOPOLITICS
TECHNOLOGY
GLOBALIZATION

Rischi dalle catene di approvvigionamento

Political disinformation
Social&economic targeting
CEO fraud

GEOPOLITICS
TECHNOLOGY

Disinformazione& ingegneria sociale

Deepfakes
Unpredictable obscure stategies

GEOPOLITICS
TECHNOLOGY
GLOBALIZATION

Intelligenza artificiale

Insiders
Untrusted third party

GEOPOLITICS
TECHNOLOGY

Mancanza di competenze

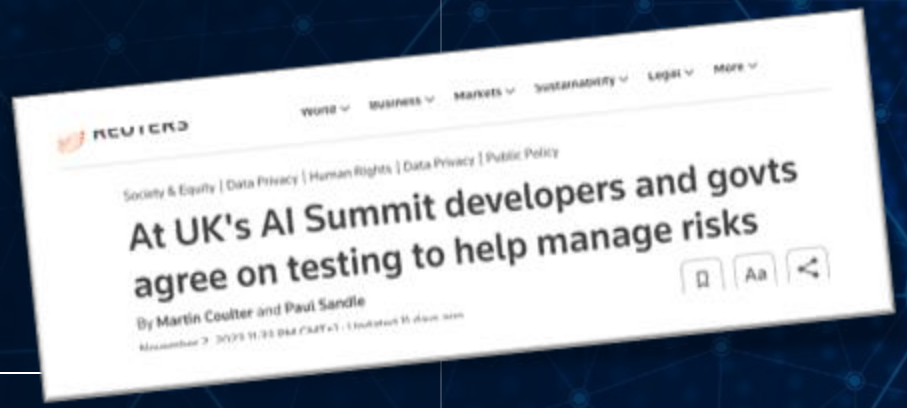
Manipolazione delle Super AI

Sicurezza vs Accuratezza nei «Large AI models»

Capire le strategie di una AI

Certificare i dati di training e gli algoritmi di «machine learning»

Monitorare le risposte dei sistemi



Rischio Cibernetico

Le società quotate in borsa comunicano annualmente informazioni sulla gestione del rischio di cybersecurity e sulle competenze dei dirigenti (luglio 2023)

SolarWinds citata in giudizio dalla SEC per aver nascosto i rischi informatici legati alla loro piattaforma Orion. (ottobre 2023)

Attacchi cyber

Rischi dalle catene di approvvigionamento

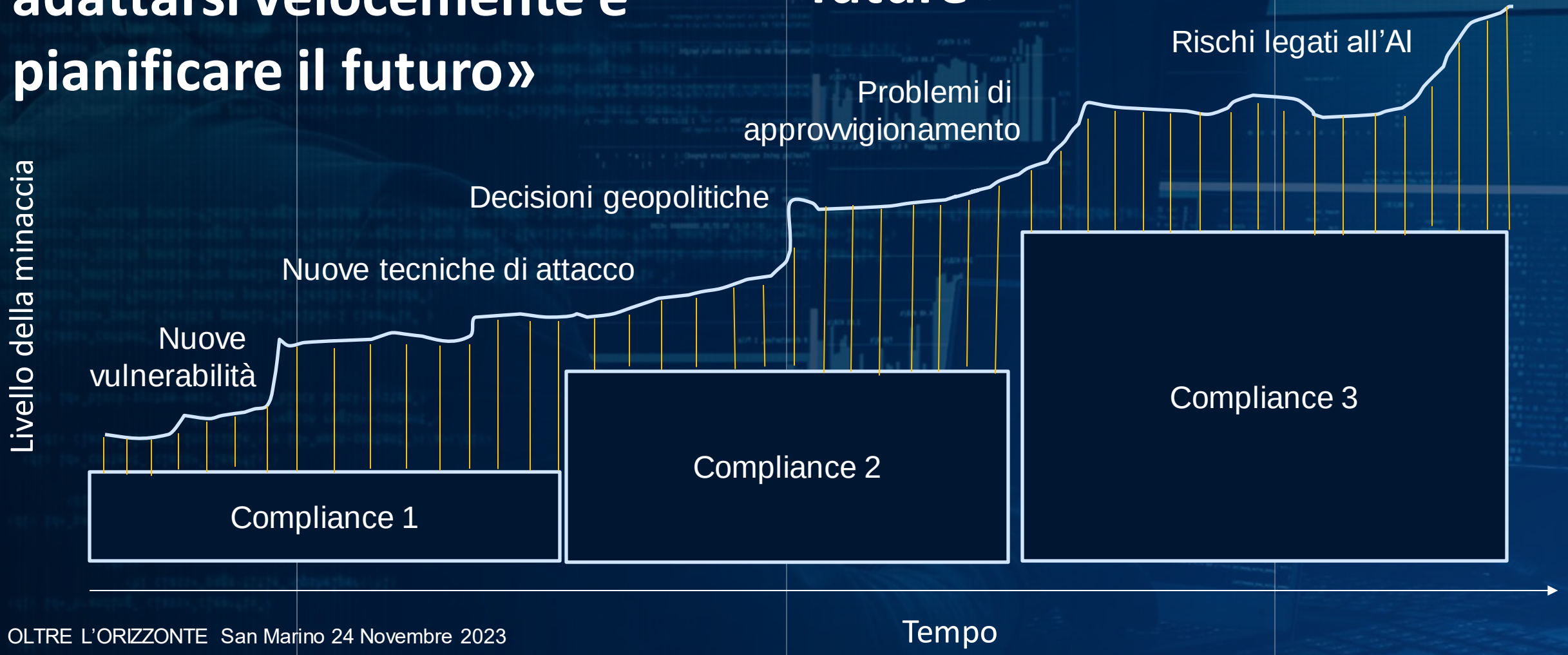
Disinformazione& ingegneria sociale

Intelligenza artificiale

Mancanza di competenze

«percepire velocemente, fondere velocemente, adattarsi velocemente e pianificare il futuro»

«sense fast, fuse fast, adapt fast and plan the future»



Quindi?

1	Compliance	
2	Day-by-day	Gestire la superficie d'attacco (personale, tecnologia e organizzazione) giorno per giorno
3	Personale	Reclutare talenti, coprire le posizioni e lavorare con terze pari fidate e con provate competenze, aiutare le azioni nazionali
4	Pensare «globale»	Ragionare considerando l'azienda un pezzo nel mosaico di complessità
5	Consapevolezza	I dipendenti sono la prima vulnerabilità aziendale e lo saranno sempre di più
6	Tecnologia	Pianificare l'acquisto di tecnologia fidata, eseguire salti tecnologici su tecnologie considerate «safe»
7	Recovery	Pensare come se ogni giorno fosse quel giorno, investire nel dopo e non solo nel day-by-day