

LA SICUREZZA E IL FUTURO INVISIBILE

**Minacce digitali, cybersecurity e disinformazione nel nuovo
disordine globale**

Prof. Marino Miculan · DMIF, Università degli Studi di Udine

Forum Democratico · I Nuovi Equilibri Globali, 3° incontro

Casarsa della Delizia, 15 ottobre 2026

Un messaggio WhatsApp da 95 milioni



Fideuram (gruppo Intesa Sanpaolo), febbraio 2026

- Il presidente riceve su WhatsApp un messaggio **dell'amministratore delegato di Intesa**: serve aiuto urgente per un'operazione all'estero.
- Segue una telefonata di un noto avvocato d'affari, **con la voce clonata dall'intelligenza artificiale**.
- Partono bonifici verso conti in Cina e Hong Kong.

95 mln €

trasferiti

53 mln €

recuperati

36 mln €

spariti in criptovalute



Il falso ministro, 2025

Voce del ministro Crosetto clonata per chiedere denaro a grandi imprenditori; una vittima paga quasi 1 milione.



La falsa figlia, Treviso

Un'anziana di 84 anni consegna 30.000 € a un truffatore che usa la voce clonata della figlia.

Perché «invisibile»?



Ieri: informazione materiale

- Coincide con il suo supporto: carta, archivi, registri
- Si protegge con mezzi fisici: serrature, casseforti, guardie
- Se viene rubata, manca qualcosa: il furto si vede



Oggi: informazione digitale

- Separata dal supporto: si copia, si sposta, si modifica in un istante
- Si attacca da qualsiasi luogo del mondo, a qualsiasi ora
- Se viene copiata, l'originale resta al suo posto: spesso ci si accorge dell'attacco dopo mesi

La transizione al digitale moltiplica le opportunità, **e con esse le possibilità di attacco.**

Più connessi, più esposti



6 miliardi

di persone online nel 2025:
circa tre quarti dell'umanità



3 miliardi

di abbonamenti 5G:
un terzo della banda larga
mobile



48.000+

nuove vulnerabilità software
pubblicate nel 2025 (+22%)

Ogni persona, dispositivo, servizio o fornitore connesso in più è **una porta in più da proteggere**: la «superficie d'attacco» cresce con la digitalizzazione.



Il quadro globale

Parte 1

Che cosa temono 1.300 esperti:
il Global Risks Report 2026
del World Economic Forum
(gennaio 2026)

The Global Risks Report 2026 21st Edition

INSIGHT REPORT



“Come vedete il mondo nei prossimi due e dieci anni?”

Turbolento o tempestoso

50%

nei prossimi
2 anni

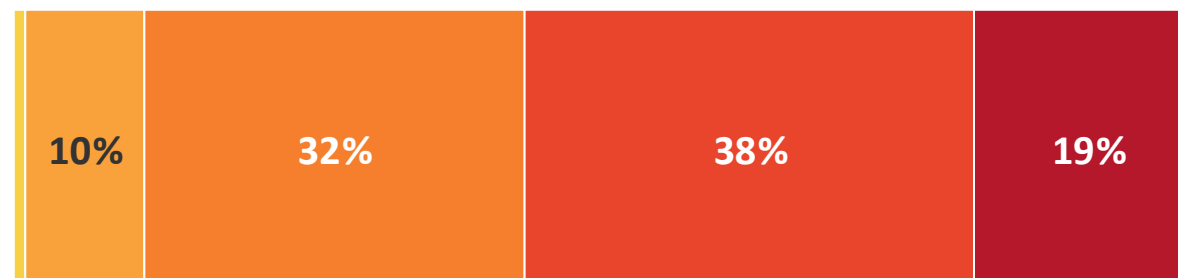
57%

nei prossimi
10 anni

Fra 2 anni



Fra 10 anni



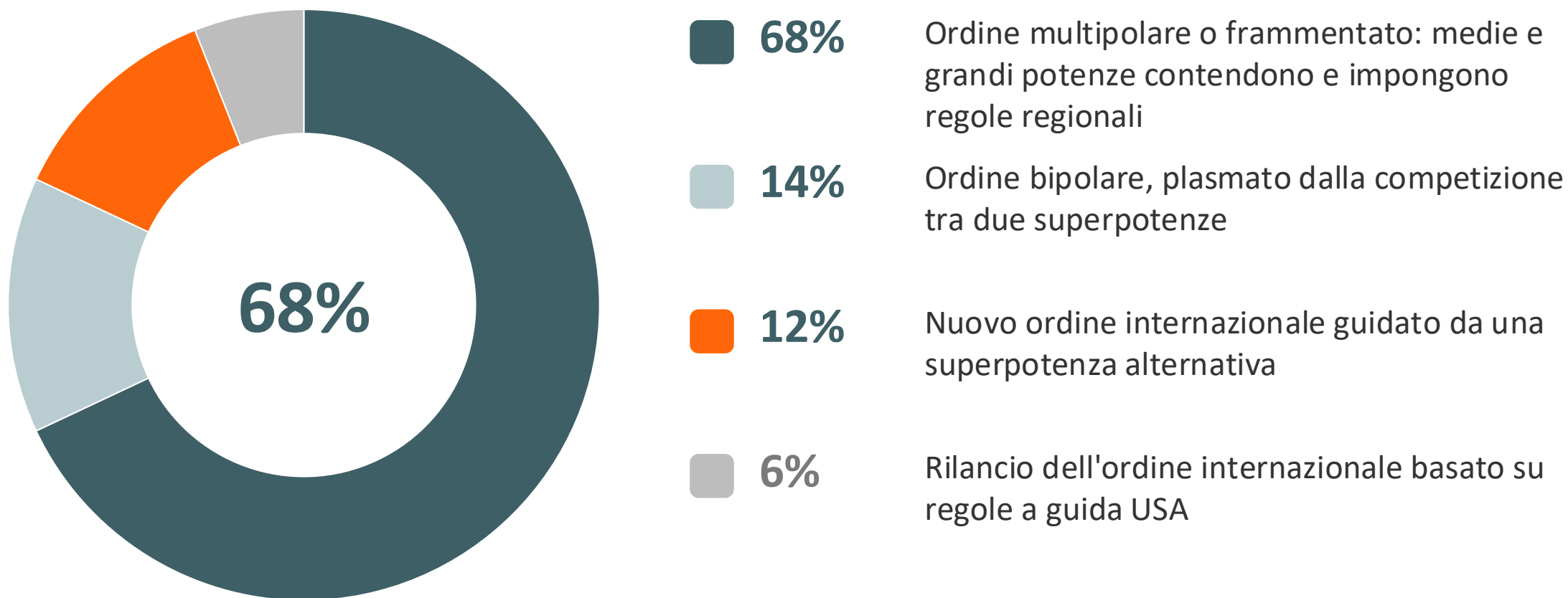
■ Calmo ■ Stabile ■ Instabile ■ Turbolento ■ Tempestoso

Rispetto al 2025, chi vede un biennio turbolento o tempestoso cresce di 14 punti.

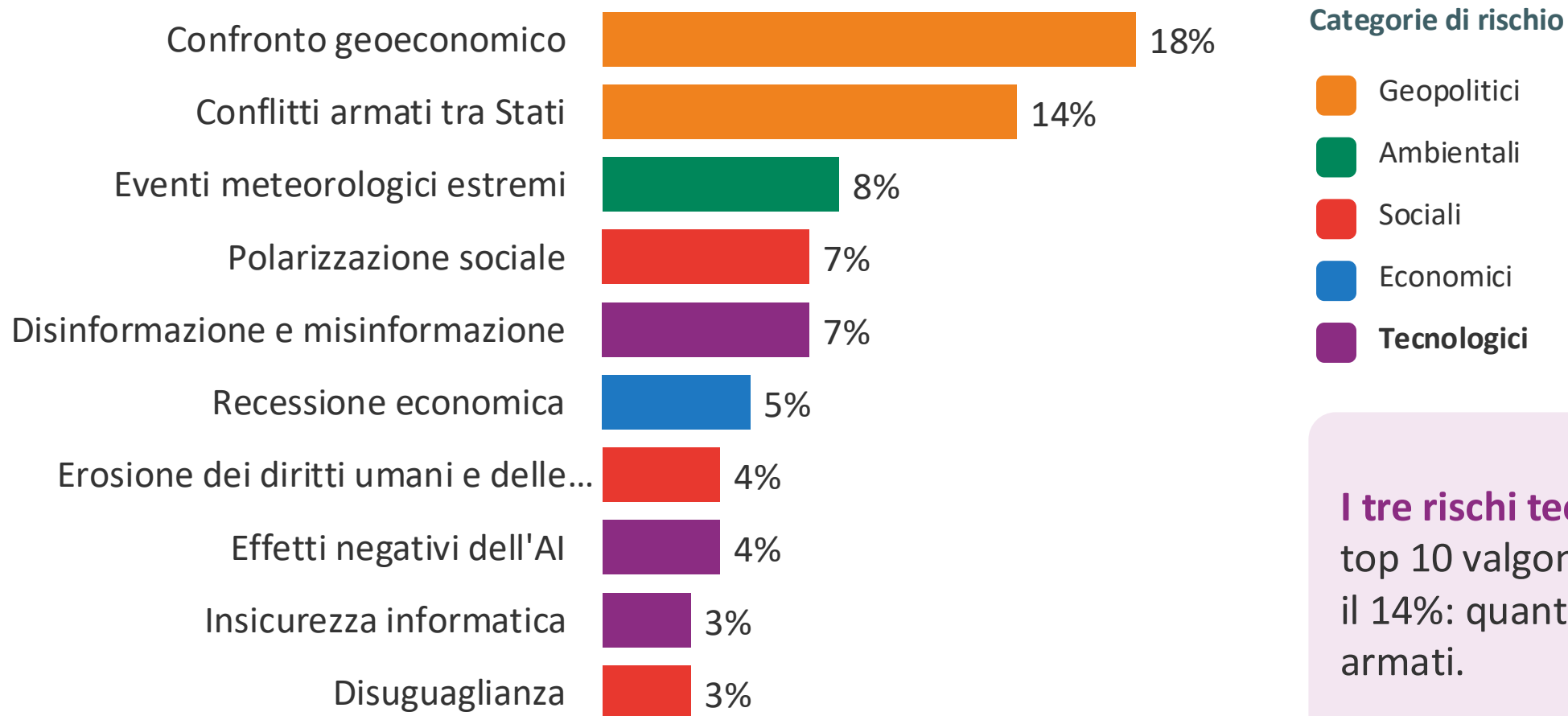
Solo l'1% prevede un mondo calmo.

L'età della competizione

Quale ordine mondiale fra 10 anni? Le risposte degli esperti interpellati dal WEF



Quale rischio può scatenare una crisi globale nel 2026?



I rischi più gravi: a 2 anni e a 10 anni

Breve termine (2 anni)



Geopolitici Ambientali Sociali

Lungo termine (10 anni)



Economici Tecnologici

I rischi digitali

Disinformazione: #2
a breve, #4 a lungo
termine

**Insicurezza
informatica: #6 e #8**

**Effetti negativi
dell'AI: dal #30 al #5.**
È il balzo più grande
tra tutti i 33 rischi.

Rischi interconnessi



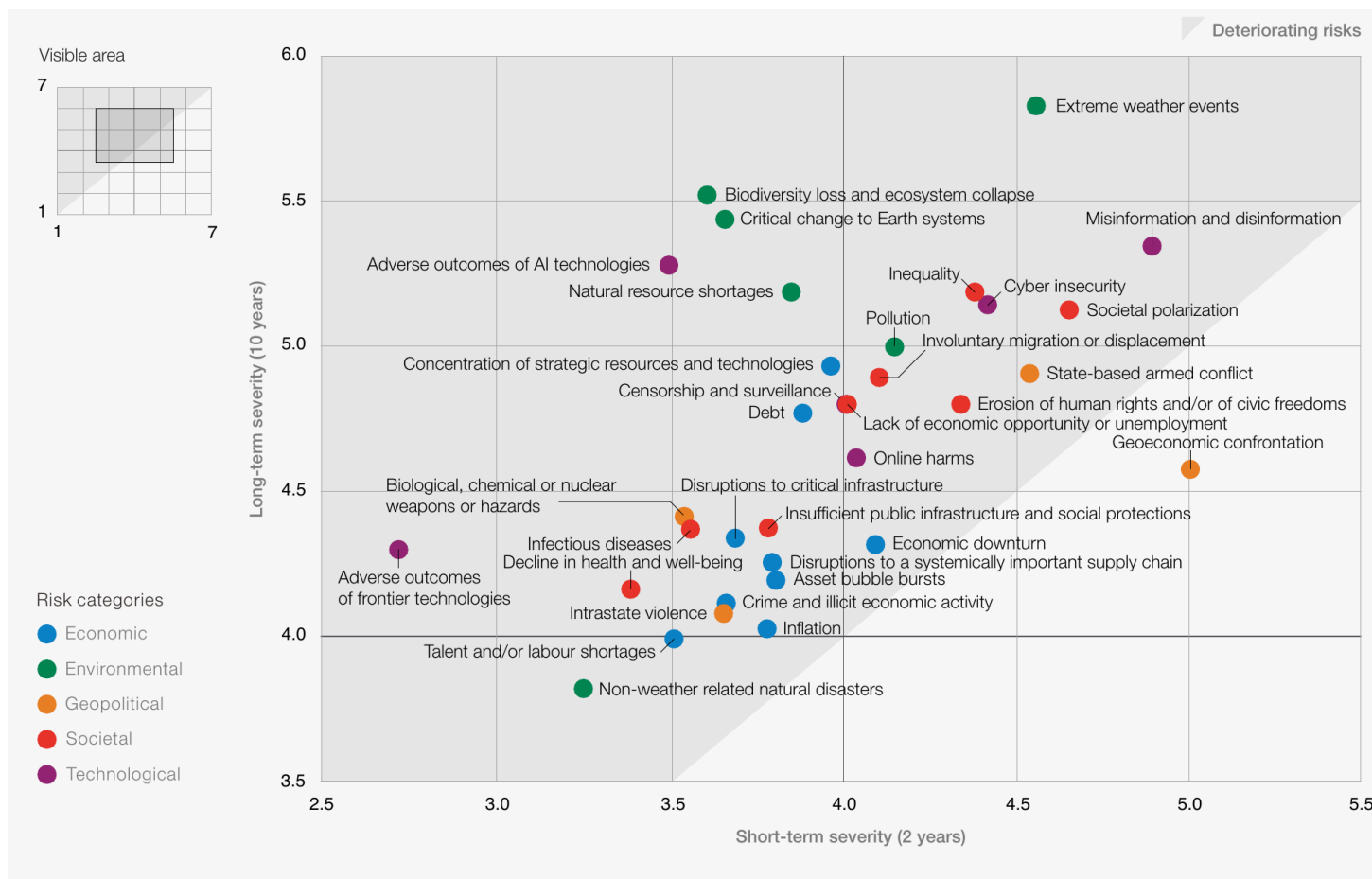
Nessun rischio è isolato: ogni crisi può innescarne altre.

La **disinformazione** (nodo viola grande) è collegata a polarizzazione sociale, erosione dei diritti e insicurezza informatica.

La **disuguaglianza** è, per il secondo anno, il rischio più interconnesso di tutti.



Gravità oggi e fra dieci anni



Asse orizzontale: gravità a 2 anni

Asse verticale: gravità a 10 anni

Area in grigio: rischi che peggioreranno

**Disinformazione e
insicurezza informatica**
restano tra i rischi più gravi
su entrambi gli orizzonti.

Effetti negativi dell'AI:
giudicati poco gravi oggi,
molto gravi domani.

E in Italia? Il rischio che non si vede

I 5 rischi principali per il Paese secondo 11.000 dirigenti d'azienda italiani

- 1 Peggioramento di salute e benessere
- 2 Mancanza di opportunità economiche o disoccupazione
- 3 Servizi pubblici e protezioni sociali insufficienti
- 4 Recessione economica
- 5 Disuguaglianza

Nessun rischio tecnologico nella top 5 italiana.

Eppure, in Europa nel 2025:

32%

degli incidenti colpisce la pubblica amministrazione, il settore più bersagliato

73%

delle organizzazioni colpite sono soggetti «essenziali» o «importanti» per la direttiva NIS2

Ciò che non si vede, si sottovaluta.

Le minacce in concreto

Parte 2

Che cosa è successo in Europa nel
2025: il Threat Landscape 2026
dell'ENISA



Europa 2025: il panorama delle minacce

51%

degli incidenti sono attacchi DDoS, per lo più di breve durata e basso impatto

57%

degli incidenti ha motivazioni ideologiche; circa il 30% punta al guadagno economico

4.709

rivendicazioni di gruppi hacktivisti contro Stati UE, per l'89% attacchi DDoS

40%

degli eventi di criminalità informatica sono attacchi ransomware

31%

sono violazioni di dati (data breach)

19%

sono frodi e furti d'identità

Il ransomware resta la minaccia con l'impatto più pesante nel breve periodo.

Chi attacca, e perché



Criminalità informatica

Movente: denaro

Ransomware, furti di dati, frodi. È il 36% degli eventi. Opera come un'industria, con servizi «a noleggio».



Hacktivisti

Movente: ideologia

Attacchi DDoS dimostrativi, legati a elezioni, proteste e tensioni geopolitiche.



Gruppi legati a Stati

Movente: spionaggio

Intrusioni silenziose e di lunga durata: la minaccia più grave nel lungo periodo.



Manipolazione informativa

Movente: influenzare

Audio, video e testi sintetici generati con l'AI, distribuiti e tradotti in massa.

I confini si fanno sempre più sfumati: criminali, attivisti e Stati usano gli stessi strumenti e le stesse infrastrutture.

Quando l'attacco esce dallo schermo



Norvegia, aprile 2025

Un attacco informatico alla diga di Bremanger provoca un rilascio d'acqua non pianificato.



Francia, ottobre 2026

Hacker portano a 50 °C i frigoriferi di centinaia di supermercati: tonnellate di cibo da buttare.



Cavi sottomarini

Cavi di telecomunicazione tagliati: Internet e finanza viaggiano sul fondo del mare.



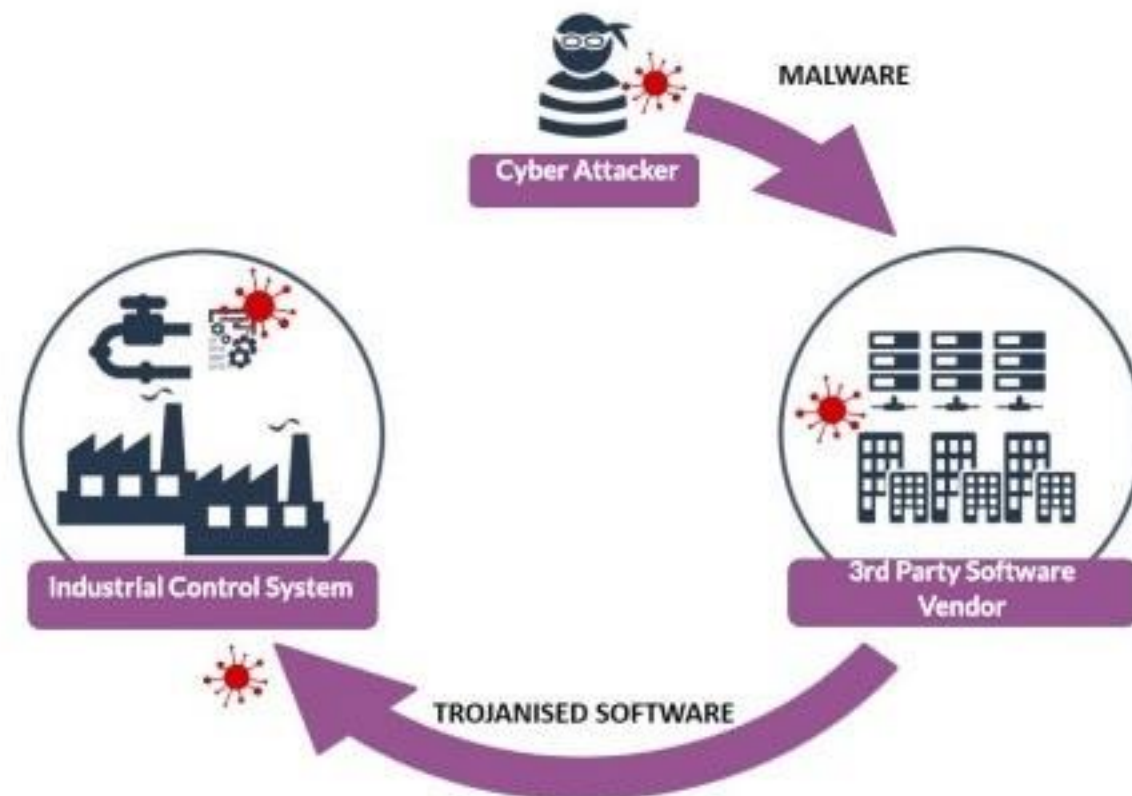
Segnali satellitari

Disturbo e falsificazione del GPS (jamming e spoofing) contro aerei, navi e logistica.

Il confine tra attacchi cyber-fisici e guerra convenzionale **potrebbe iniziare a sfumare.** (WEF)

Imprese: l'anello debole è il fornitore

- **Si attacca un fornitore** (software, servizi, cloud) per raggiungere tutti i suoi clienti in un colpo solo
- **Le «dipendenze digitali»** allargano la superficie d'attacco e causano gli incidenti più estesi (ENISA)
- **Crescono i componenti software compromessi** nelle librerie open source usate da milioni di programmi
- **Il ransomware** unisce cifratura, furto di dati ed estorsione



Cittadini: la truffa ha la voce di chi conosci



Phishing evoluto

Messaggi credibili e senza errori, scritti con l'AI. Nuove tecniche come «ClickFix»: finte schermate di verifica che inducono a eseguire comandi sul proprio computer.



Voci e volti clonati

Deepfake audio e video: il familiare in difficoltà, il direttore di banca, il personaggio famoso che «consiglia» un investimento.



Falsi siti di notizie

Pagine che imitano testate note per promettere guadagni facili. Le frodi sugli investimenti online sono costate circa 4 miliardi di euro nello Spazio economico europeo nel 2024.

Il punto d'attacco non è il computer: siamo noi. Fretta, paura e fiducia sono le leve.

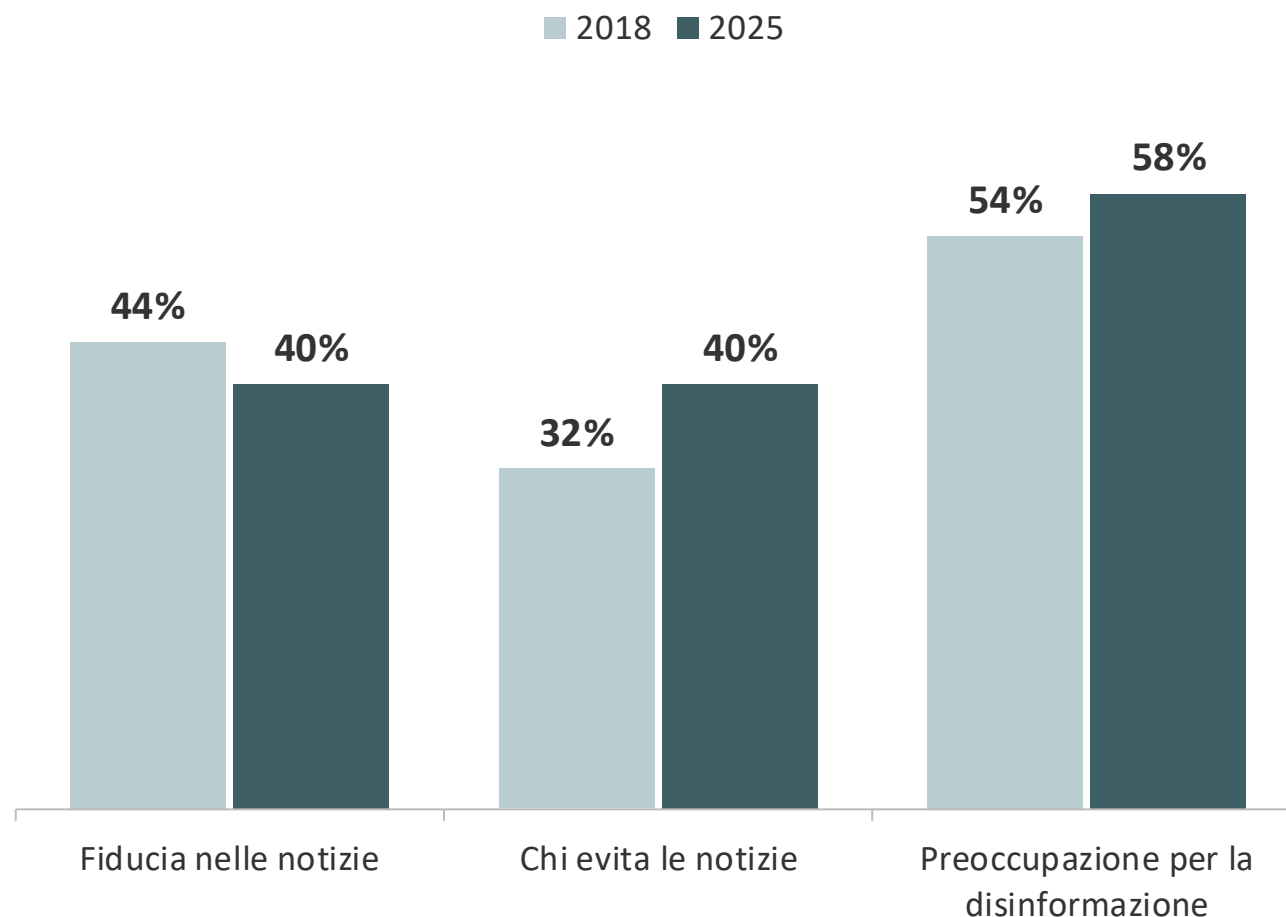
Disinformazione e democrazia

Parte 3

Quando il bersaglio è la fiducia:
notizie, elezioni, istituzioni



Fiducia in calo, preoccupazione in aumento



58%

teme di non saper distinguere il vero dal falso nelle notizie online (73% negli USA)

4% → 34%

americani che si informano soprattutto sui social (2015 → 2025)

11% → 24%

chi usa l'AI per cercare informazioni (2024 → 2025)

Deepfake ed elezioni

- **Creare un deepfake** è diventato più facile, economico e convincente
- **Contenuti fabbricati** hanno segnato le recenti elezioni in USA, Irlanda, Paesi Bassi, Pakistan, Giappone, India e Argentina
- **Nel Regno Unito l'87%** teme che i deepfake influenzino i risultati elettorali, ma pochi si sentono capaci di riconoscerli
- **Rischio:** sfiducia nelle istituzioni, polarizzazione, fino all'incitamento alla violenza



Romania, dicembre 2024

La Corte costituzionale annulla il primo turno delle presidenziali, dopo che i servizi di intelligence documentano una campagna di influenza coordinata su TikTok.

In Europa la disinformazione è tra i primi 3 rischi nazionali indicati dai dirigenti d'azienda; nel mondo è in top 10 in 67 Paesi.

Anatomia di una campagna di manipolazione



FIMI (manipolazione e interferenza informativa straniera): comportamento intenzionale e coordinato, spesso di attori statali, che minaccia valori e processi democratici.

Per lo più non è illegale: per questo è così difficile da contrastare.

Il futuro invisibile

Parte 4

Intelligenza artificiale e computer
quantistici: i rischi che si stanno
preparando oggi



Intelligenza artificiale: il rischio che cresce di più

Posizione nella classifica WEF

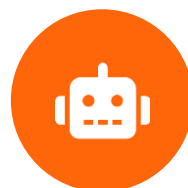
#30 → #5

da 2 a 10 anni

Mercato globale dell'AI

280 mld \$ (2024)

3.500 mld \$ (stima 2033)



Uno strumento per chi attacca

L'ENISA prevede che nel 2026 sempre più fasi degli attacchi saranno direttamente svolte dall'AI.



Un nuovo bersaglio

I sistemi di AI integrati in aziende e amministrazioni allargano la superficie d'attacco.



Un rischio militare

Con l'AI nei sistemi di comando, crisi che duravano giorni potrebbero degenerare in pochi secondi.

Il computer quantistico: «raccogli ora, decifra dopo»

**Oggi**

I dati cifrati vengono rubati e conservati: cartelle cliniche, segreti industriali, comunicazioni riservate.

**Q-Day**

Arriva un computer quantistico abbastanza potente da rompere la crittografia asimmetrica attuale (RSA).

**Domani**

I dati rubati anni prima diventano leggibili; le identità digitali e le firme diventano falsificabili.

53%

degli esperti stima almeno 50% di probabilità che entro 10 anni si possa rompere RSA-2048 in 24 ore

5%

soltanto delle organizzazioni ha già adottato una cifratura resistente ai computer quantistici

2024

il NIST pubblica i primi standard di crittografia post-quantistica; l'UE ha una tabella di marcia

Che cosa possiamo fare

Parte 5

Istituzioni, imprese, cittadini: la
sicurezza è una responsabilità
condivisa



La sicurezza non si compra: è un ciclo continuo

Governare: i vertici fissano priorità, regole e risorse, e ne rispondono



Identificare

Che cosa abbiamo, che cosa rischiamo



Proteggere

Accessi, aggiornamenti, cifratura, formazione



Rilevare

Accorgersi presto che qualcosa non va



Rispondere

Contenere l'attacco, avvisare chi serve



Ripristinare

Tornare operativi dai backup e imparare



e si ricomincia

Conoscere chi attacca

Chi può colpirci, perché, che cosa cerca

Spendere il giusto

In proporzione al valore da proteggere e ai danni possibili

Persone preparate

Servono competenze specialistiche, oggi scarse: non ci si improvvisa

Istituzioni e imprese: chi fa che cosa



Istituzioni

- **Regole comuni:** direttiva NIS2 e Perimetro di sicurezza nazionale cibernetica (obblighi di protezione e di notifica degli incidenti)
- **Coordinamento:** Agenzia per la Cybersicurezza Nazionale, cooperazione europea, partenariato pubblico-privato
- **Infrastrutture:** monitorare i sistemi industriali e pianificare la migrazione alla crittografia post-quantistica
- **Informazione:** trasparenza e alfabetizzazione digitale contro la disinformazione



Imprese

- **Continuità:** la sicurezza non è un prodotto, è un processo che non si ferma
- **Rischio:** valutarlo con regolarità e decidere dove investire
- **Cultura:** formazione di tutto il personale, a partire dai vertici
- **Fornitori:** conoscere e verificare le proprie dipendenze digitali
- **Resilienza:** backup, piani di risposta e competenze specialistiche (che oggi mancano)

Per tutti: Otto gesti di igiene digitale



Attivare l'autenticazione a due fattori

su posta, banca e social



Aggiornare sempre

telefono, computer, router e
app



Fare copie di backup

regolari, anche su un disco
scollegato



Usare password diverse

meglio con un gestore di
password



Diffidare dell'urgenza

chi mette fretta, di solito,
mente



Richiamare su un numero noto

banca, ufficio, familiari: mai
quello ricevuto



Una parola d'ordine in famiglia

per smascherare le voci
clonate



Verificare prima di condividere

chi lo dice? quando? dove
altro è scritto?

Prima riga: proteggere i dispositivi. **Seconda riga:** proteggere noi stessi dall'inganno.

*Non illuderti che il nemico possa
non venire, ma tieniti sempre
pronto ad affrontarlo. Non
illuderti che il nemico non ti
attacchi, ma fai piuttosto in modo
di renderti inattaccabile*
— Sun Tzu, L'arte della guerra



La sicurezza è un bene comune

- Invisibile non vuol dire inevitabile.
- La tecnologia da sola non basta: servono regole, competenze e cultura.
- Difendere l'informazione è difendere la democrazia.

Grazie

marino.miculan@uniud.it • marino.miculan.org