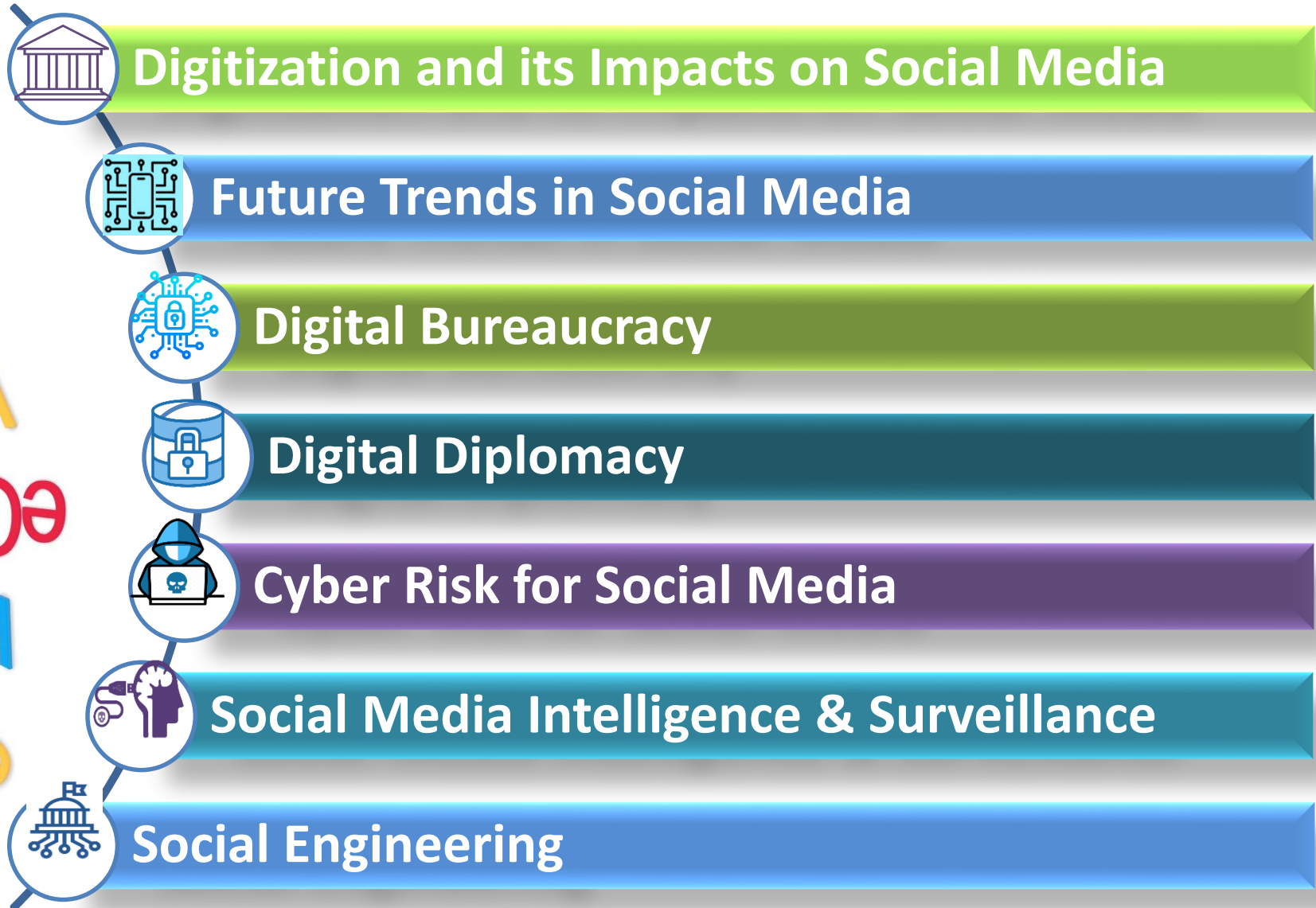


Media...Future of Social Media





Education

B.Tech., MBA

Experience

20 Years of IT Experience of which 10 with Cyber Defense, Threat Intelligence, Telecom Intelligence & Digital Transformation.

Certification

ISO27001

ISO 22301 LI

CoBIT5

TOGAF 9

Prince2

CBCI (BCM)

MCITP

CCNA

Oracle Big Data

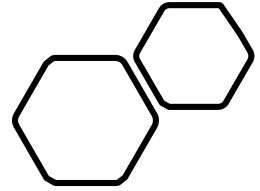
Oracle Virtualization

Oracle DB12

Oracle GTM

Expertise

Cyber Risk Advisor to the Governments, PSU's & Critical Infrastructure Entities



Our

Companies



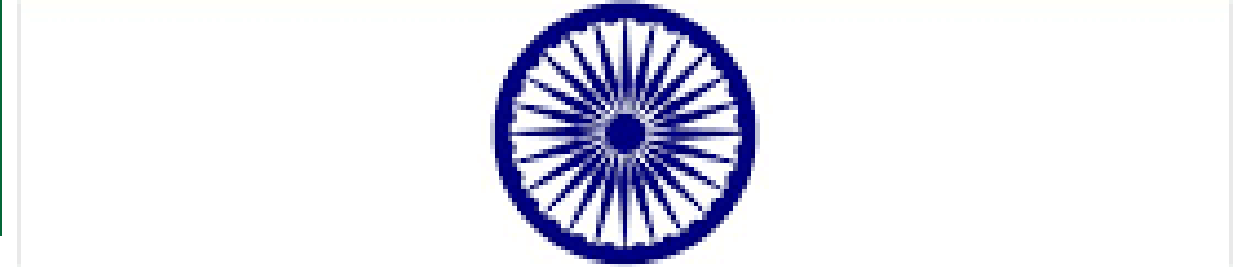
HUNTMETRICS

PV

PRIVACY VIRTUOSO



ALLIANCE PRO



Strategic Customers



قطر تستحق الأفضل
Qatar Deserves The Best

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT
AND COMMUNICATIONS



اللجنة العليا
للمشاريع والورث
Supreme Committee
for Delivery & Legacy



وزارة المالية
MINISTRY OF FINANCE



بنك قطر الأول
QFB



جهاز قطر للإستثمار
QATAR INVESTMENT AUTHORITY



قطر للبترول
Qatar Petroleum



بنك الدوحة
DOHA BANK



بنك بروة
BARWA BANK



QNB
Qatar National Bank



بنك قطر للتنمية
QATAR DEVELOPMENT BANK



البنك الأهلي
ahlibank



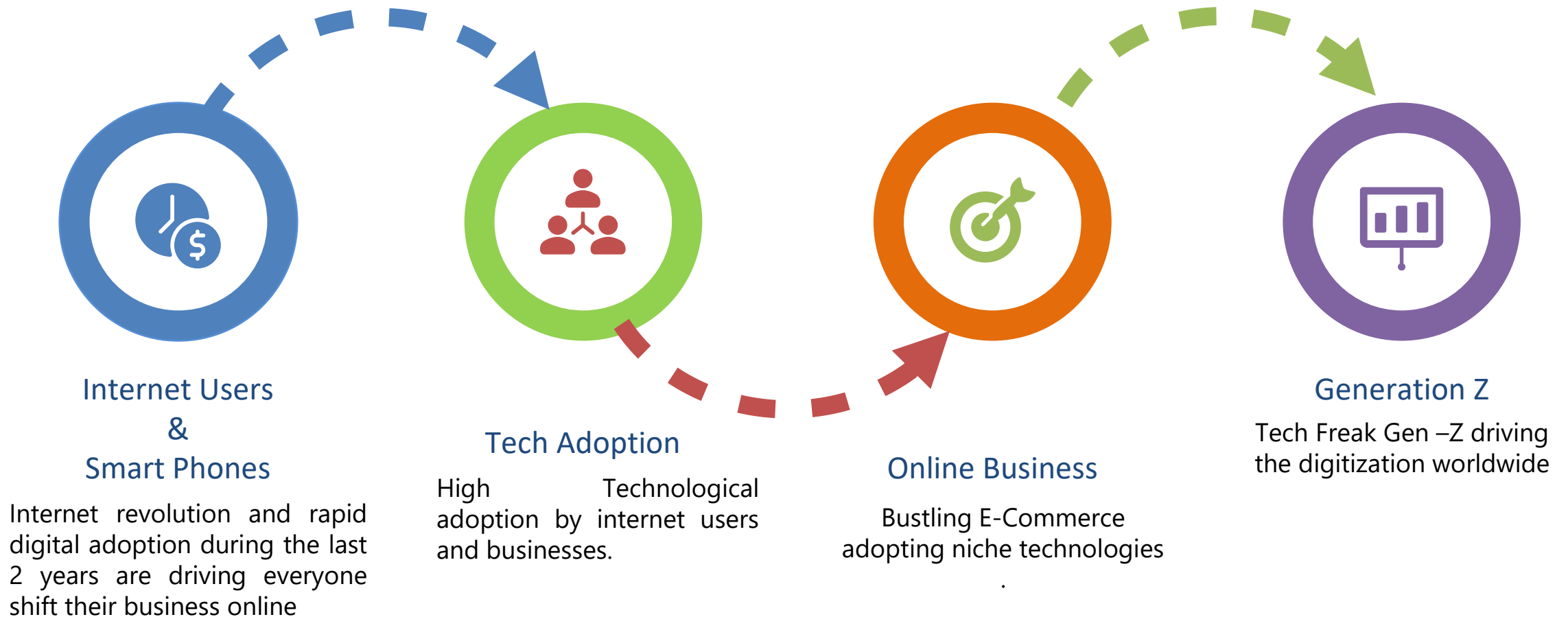
شركة قطر البتروكيماويات
QATAR PETROCHEMICAL COMPANY



ناقلات
NAKILAT

Digitalization Factors

The implications of COVID-19 have accelerated digital adoption. The increasing use of technology to work, play, and stay connected have shaped new digital habits.



APR
2022

ESSENTIAL DIGITAL HEADLINES

OVERVIEW OF THE ADOPTION AND USE OF CONNECTED DEVICES AND SERVICES



TOTAL
POPULATION



we
are
social

7.93
BILLION

URBANISATION

57.0%

UNIQUE MOBILE
PHONE USERS



5.32
BILLION

vs. POPULATION

67.0%

INTERNET
USERS



5.00
BILLION

vs. POPULATION

63.0%

ACTIVE SOCIAL
MEDIA USERS



4.65
BILLION

vs. POPULATION

58.7%

FEB
2022

ESSENTIAL DIGITAL HEADLINES

OVERVIEW OF THE ADOPTION AND USE OF CONNECTED DEVICES AND SERVICES



INDIA

TOTAL
POPULATION



1.40
BILLION

URBANISATION

35.9%

CELLULAR MOBILE
CONNECTIONS



1.14
BILLION

vs. POPULATION

81.3%

INTERNET
USERS



658.0
MILLION

vs. POPULATION

47.0%

ACTIVE SOCIAL
MEDIA USERS



467.0
MILLION

vs. POPULATION

33.4%

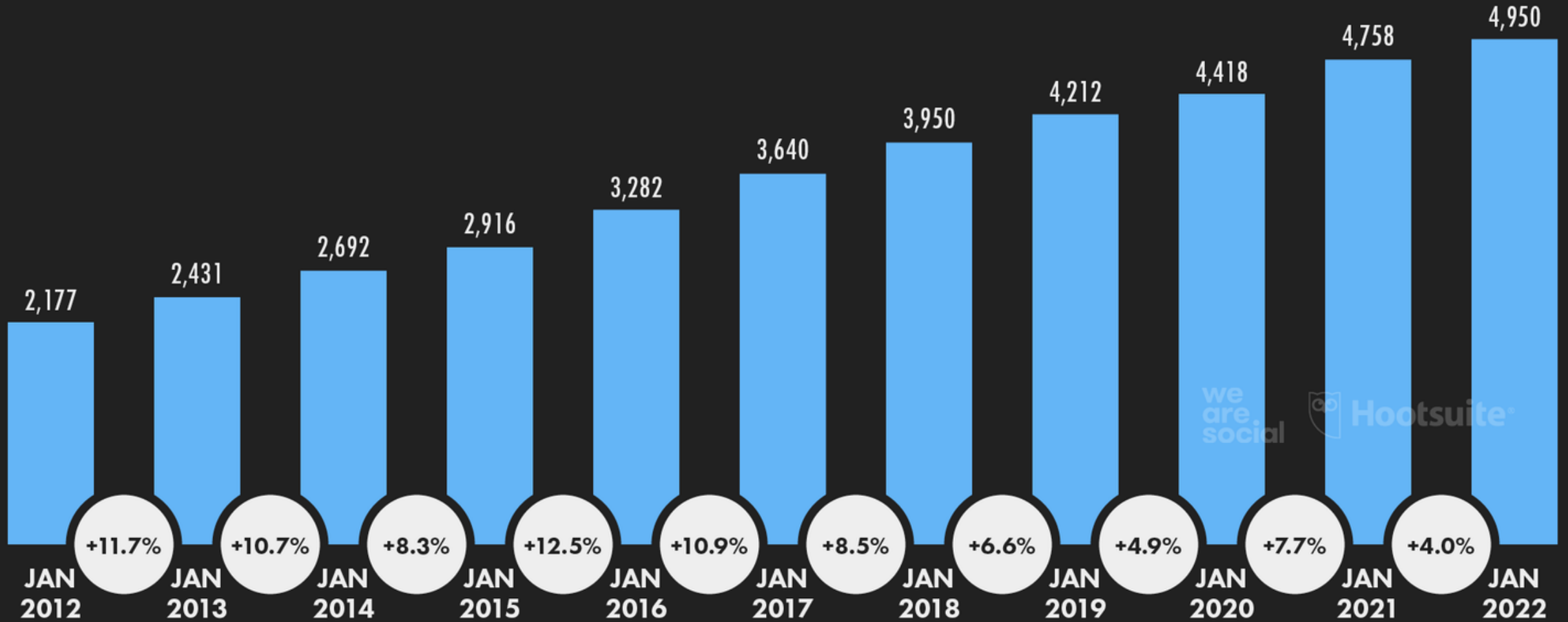


SOURCES: UNITED NATIONS, U.S. CENSUS BUREAU, GOVERNMENT BODIES, GSM.A INTELLIGENCE, ITU, G.W, EUROSTAT, ONNIC, A.B.I, CIA WORLD FACTBOOK, COMPANY ADVERTISING RESOURCES AND EARNING'S REPORTS, OECD, TECHRASA, KEPIOS ANALYSIS. **ADVISORY:** SOCIAL MEDIA USERS MAY NOT REPRESENT UNIQUE INDIVIDUALS. **COMPARABILITY:** SOURCE AND BASE CHANGES.

JAN
2022

INTERNET USERS OVER TIME

NUMBER OF INTERNET USERS (IN MILLIONS) AND YEAR-ON-YEAR CHANGE



SOURCES: KEPIOS ANALYSIS; ITU; GSMA INTELLIGENCE; EUROSTAT; GWI; CIA WORLD FACTBOOK; CNNIC; APJII; LOCAL GOVERNMENT AUTHORITIES. **ADVISORY:** DUE TO COVID-19-RELATED DELAYS IN RESEARCH AND REPORTING, FIGURES FOR INTERNET USER GROWTH AFTER 2020 MAY UNDER-REPRESENT ACTUAL TRENDS. SEE [NOTES ON DATA](#) FOR MORE DETAILS. **COMPARABILITY:** SOURCE AND BASE CHANGES. FIGURES MAY NOT MATCH OR CORRELATE WITH FIGURES PUBLISHED IN PREVIOUS REPORTS.



What is Metaverse

Metaverse is an augmented reality platform that allows users to create interactive experiences that merge the digital world with the physical world.

How to Enter Metaverse

<https://decentraland.org/>

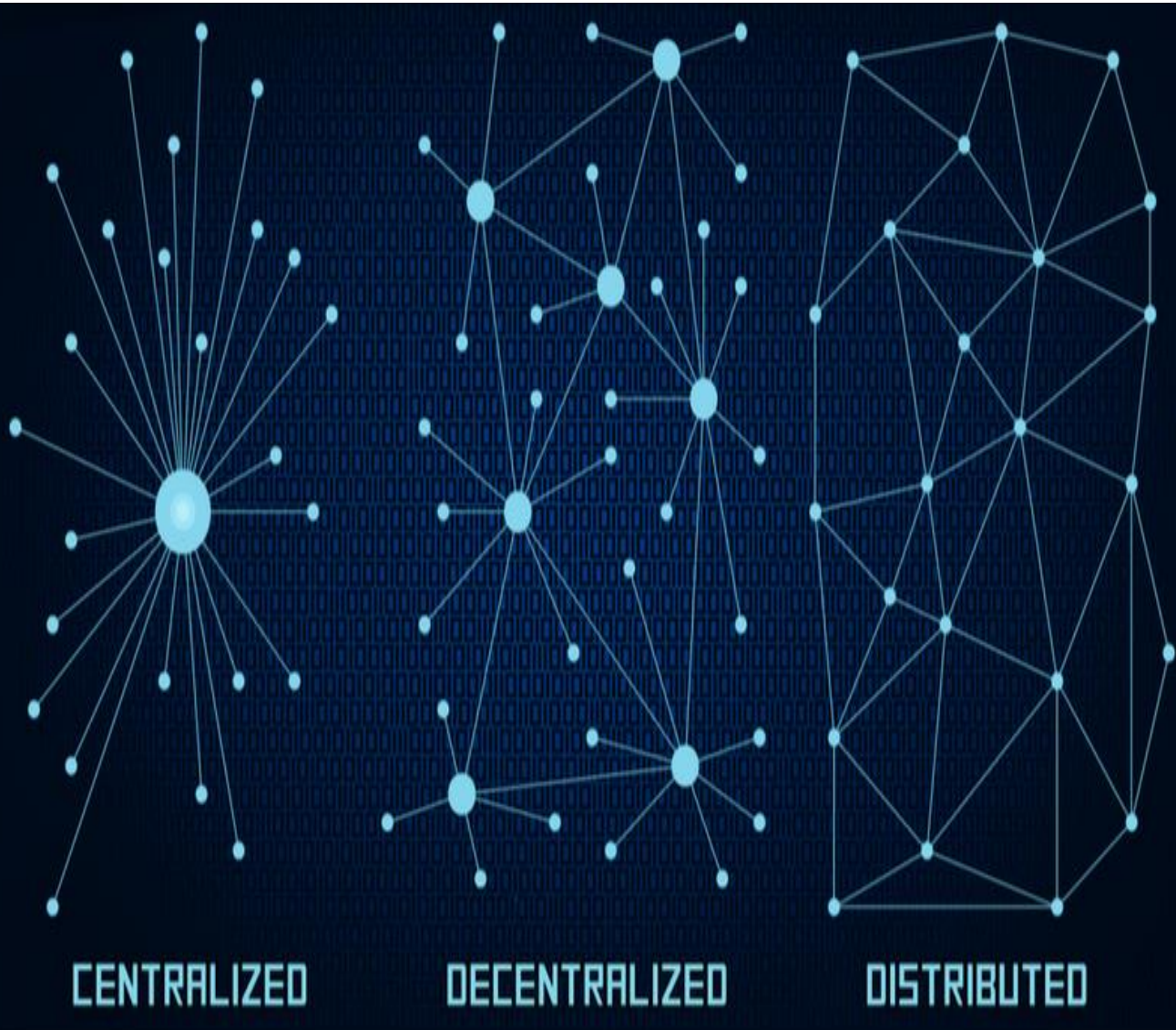
- Create an Avatar
- Explore the virtual world
- Play games
- Attend Events
- Connect with new friends
- Invest on Virtual real estates
- Trade business using crypto currencies
- Build Business
- Create NFT and Trade

DeepFakes

- Deepfake is a type of artificial intelligence used to create convincing images, audio and video hoaxes.
- Spread misinformation and inspire misunderstanding, fear or mislead.
- Create false narratives of people or group
- Create revenge porn to impact their integrity.
- Generate a specific public image for the subject (and sometimes make a one of themselves that contrasts and depends on the subject's falsified public image)
- Censure or mock the subject for deception
- Societal unrest

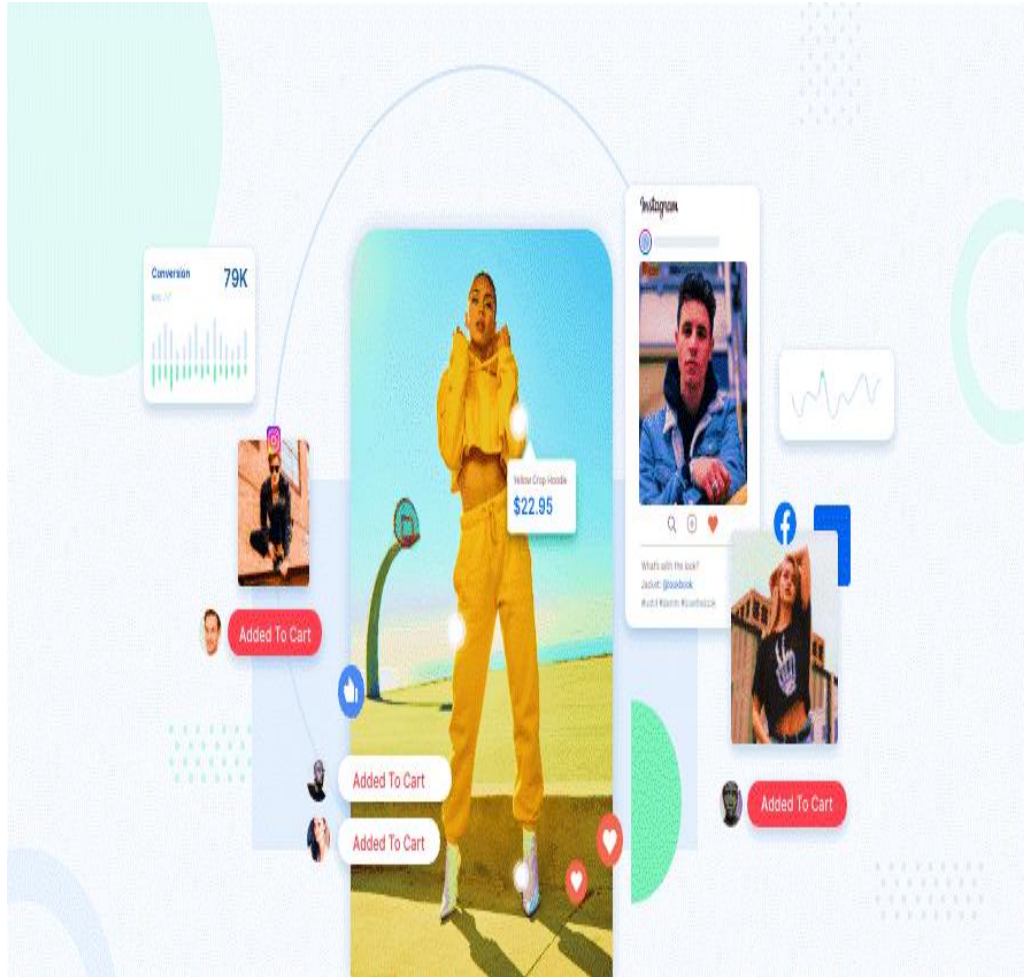


Decentralized Network



- **Centralized Network:** is controlled by a single admin. A single authority will have all the controls through a single central server.
- **Decentralized Network:** In this whole network will be distributed, Every node in the network will work as an individual authority. These nodes have their own decision-making powers.
- **Distributed Network:** In this no one needs to know or trust anyone else. Each member in the network has a copy of the exact same data in the form of a distributed ledger. If a member's ledger is altered or corrupted in any way, it will be rejected by the majority of the members in the network

Social Commerce



- Social commerce is the use of social media platforms to promote and sell products and services. It encourages and allows users to buy products directly within social media platforms, never having to open another browser
- **The Six Pillars Of Social Commerce**
 1. Buyers' community (GDGT)
 2. Group buying (Groupon, Living social)
 3. Purchase sharing (JustBoughtIt)
 4. Curation (Polyvore, Pinterest)
 5. Social advice (Fashism)
 6. Co-shopping

Predictive Analytics



- In social media, predictive models bring out customer patterns derived from the historical and transactional data to identify risks and opportunities.
- Few types of predictive analytics in social media
 1. Performance metrics
 2. Audience analytics
 3. Competitor analytics
 4. Paid social analytics
 5. Influencer analytics
 6. Sentiment analysis
 7. Behavior Analytics

Multi Sensory Social Media



- Multi-sensory marketing is the art and science of engaging our senses holistically. Research demonstrates that if we trigger a response from two of your customer's senses, such as sound and visual, a customer's experience is enhanced, and brand engagement is multiplied.
- **The five basic sensory systems:**
 1. Visual.
 2. Auditory.
 3. Olfactory (smell) System.
 4. Gustatory (taste) System.
 5. Tactile System.

Digital Bureaucracy



DIGITAL
BUREAUCRACY

Government production is based on bureaucracy. The classic bureaucracy is challenged by a shift from paper-based to digitized information, the shift also offers transparency, significant productivity gains, and more efficient service delivery.

Pros:

- Enhances the access of the civil servants for the people
- created a positive outlook towards an institution long perceived as opaque and inaccessible.
- increased awareness among people about government policies and programs.
- opportunity for the bureaucrats to shape the public discourse and engage with the public while being politically neutral.
- created an effective system where we could get citizens' feedback in a seamless manner

Advantages



Connect

- Create engaging posts, photos and videos.
- Conduct Survey for the audience.



Engage

- Receive feedback from an audience.
- Listen to opinions and commentary on issues.



Manage

- Real time Situational Awareness
- Understand the pulse of the people

Digital Diplomacy



Digital diplomacy refers to the impact of digital technology on diplomacy in three realms:

- Changing digital geopolitical and geo-economic environment for diplomatic activities (sovereignty, power redistribution, interdependence)
- Emerging digital TOPICS on diplomatic agenda (e.g., cybersecurity, e-commerce, privacy protection, and
- New TOOLS for diplomatic activities (e.g., social media, big data, AI).

Digital Diplomacy Goals




“Huh. So Iran just friended us on Facebook ... Like, do I accept?”

Goals of Digital Diplomacy

- Public Diplomacy
- Knowledge Management
- Information Management
- Consular communication & Response
- Disaster Response
- Rescue Operations
- Internet Freedom
- Policy Planning
- External Resource

Types of Cyber Attack

1 Malware
●●●



TREND

2 Web based attacks
●●●



TREND

3 Web application attacks
●●●



TREND

4 Phishing
●●●



TREND

5 Spam
●●



TREND

6 Denial of service
●●●●




TREND

7 Ransomware
●●●



TREND

8 Botnets
●



TREND

9 Insider threat
●●●●●●●



TREND

10 Physical manipulation damage / theft / loss
●●



TREND

11 Data breaches
●●●



TREND

12 Identity theft
●●●●



TREND

13 Information leakage
●●●●●



TREND

14 Exploit kits
●●●●



TREND

15 Cyber espionage
●●●●●



TREND

KILL CHAIN

● Reconnaissance ● Weaponisation ● Delivery ● Exploitation ● Installation ● Command and Control ● Actions on Objectives

Global Cybercrime Damage Costs:

- **\$6 Trillion USD a Year.** *
- **\$500 Billion a Month.**
- **\$115.4 Billion a Week.**
- **\$16.4 Billion a Day.**
- **\$684.9 Million an Hour.**
- **\$11.4 Million a Minute.**
- **\$190,000 a Second.**



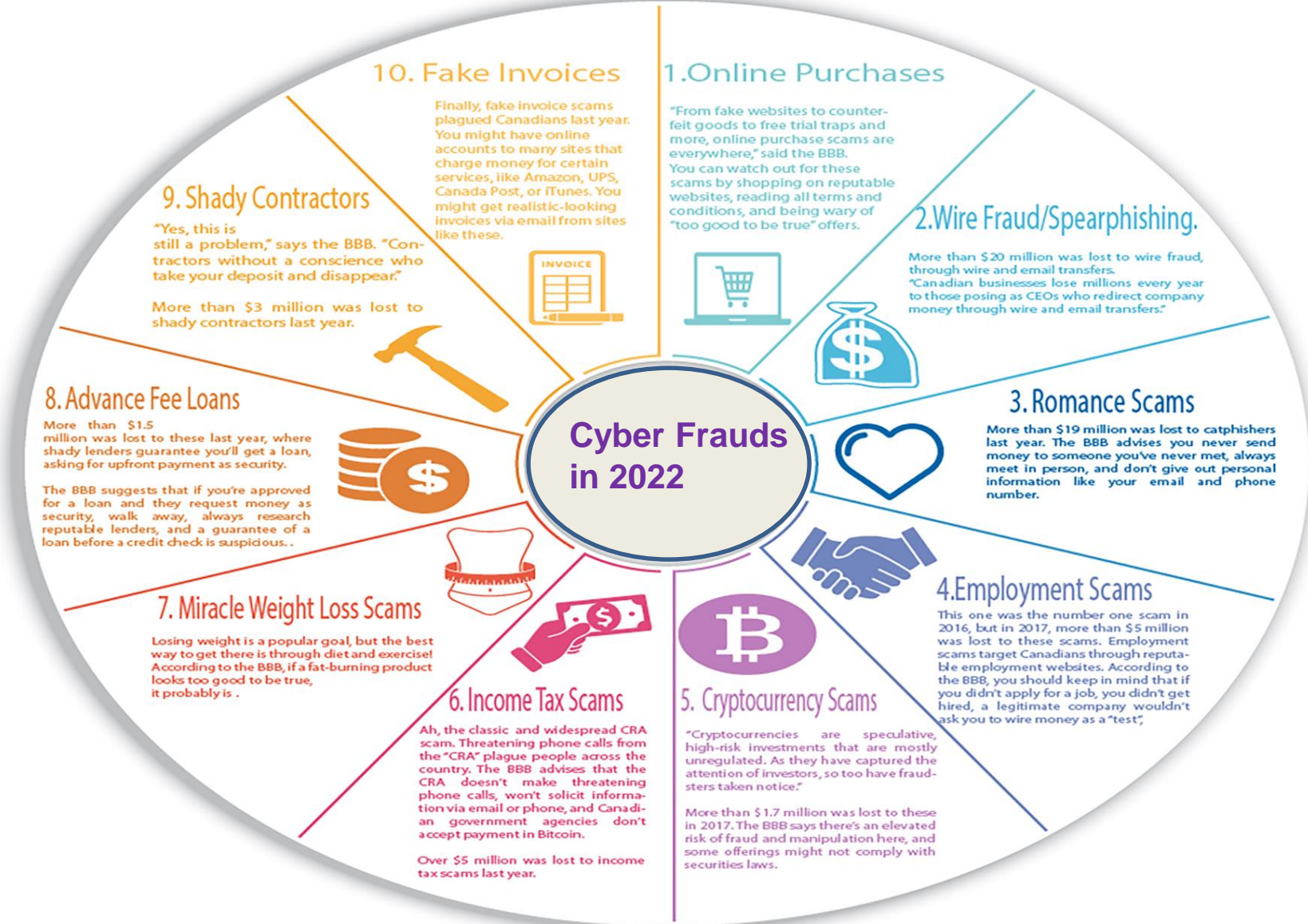
ALL FIGURES ARE
PREDICTED BY 2021

* SOURCE: CYBERSECURITY VENTURES



**CYBERSECURITY
VENTURES**

Online Fraud Trends



Social Media Surveillance



Social Media Intelligence

Introduction/ Social Media Intelligence Cycle

TARGETS

- What problems do we have?
- What information do we need?
- What departments should be included?

ENGAGEMENT

- Speak to your customers
- Drive new business
- Encourage repeat sales

ANALYSIS

- Analysis of the results
- Recommendations and action plans
- Performance measurement & optimisations

Social Media Intelligence Cycle

FILTERING

- Structuring the data
- Filters: channels, topics, authors, countries, time, sentiment etc.

TOOL SELECTION

- Finding a suitable Monitoring tool
- How broad is their coverage?
- How deep can you dive into the data?
- What metrics can they analyse?
- What additional services (support) do they offer?

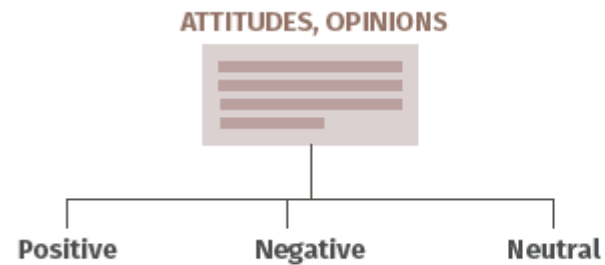
GATHERING DATA

- Creating queries for brand / product / topics /market
- Gathering relevant data

Social Media Analysis

SENTIMENT ANALYSIS

Sentiment analysis refers to the class of computational and natural language processing study of people's opinions, appraisals, and emotions toward events, institutions or other subject matter in order to extract subjective information, such as opinions, expressed in a given piece of text.

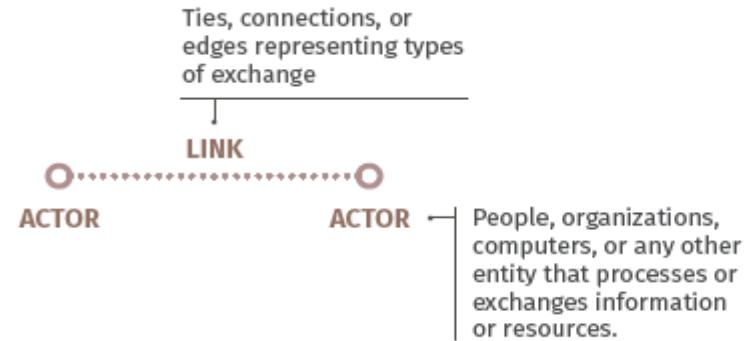


CATEGORIES

- Document Level Analysis
- Sentence Level Analysis
- Aspect Based Analysis
- Comparative Analysis

SOCIAL NETWORK ANALYSIS

Social network analysis is a technique used to map and measure social relations. They are used in investigative tools to discover, analyze, and visualize the social networks of criminal suspects.



Centrality Analysis

Centrality analysis aims at determining more important actors of a social network so as to understand their prestige, importance, or influence in a network.

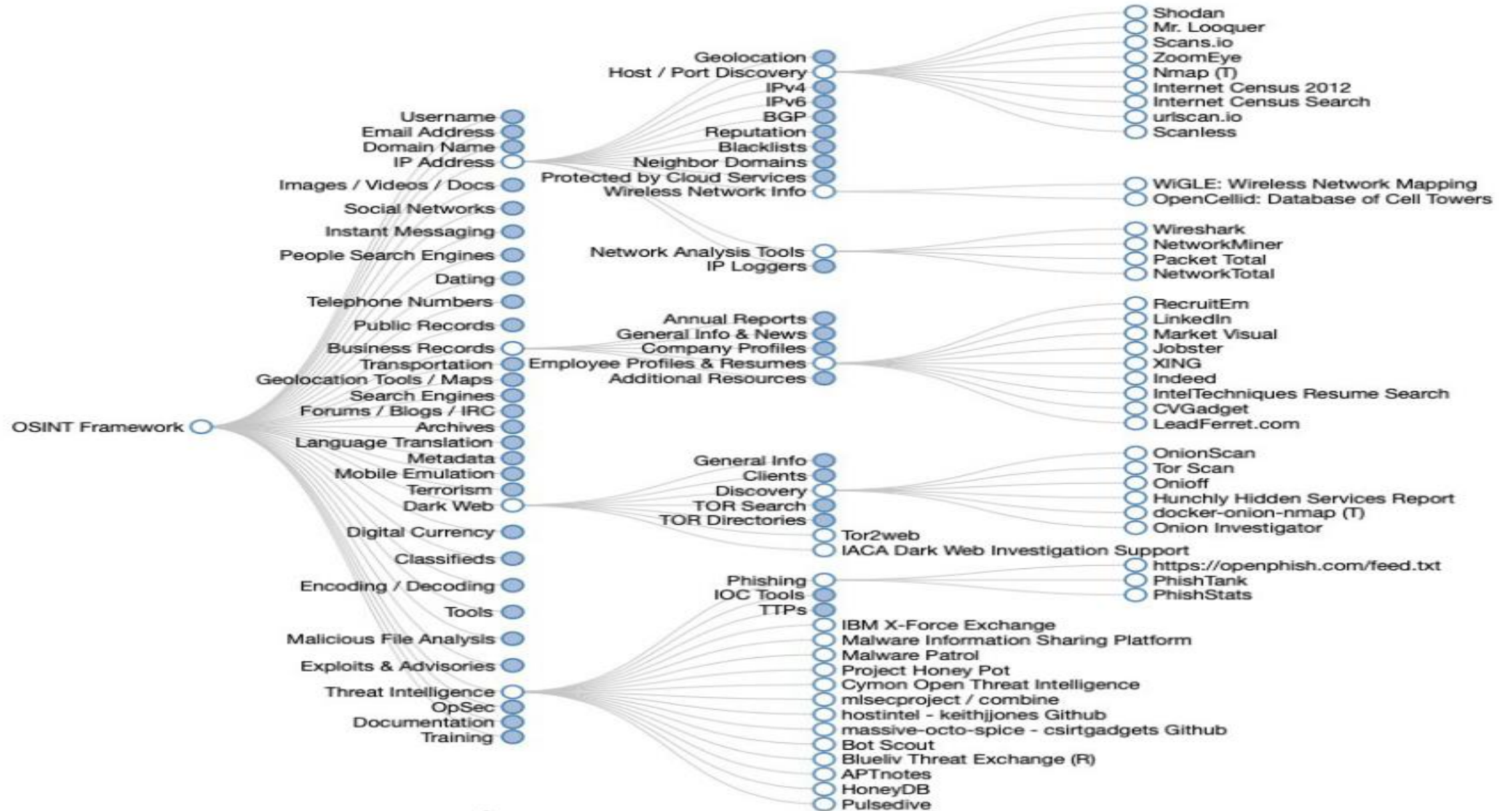


Community Detection Methods

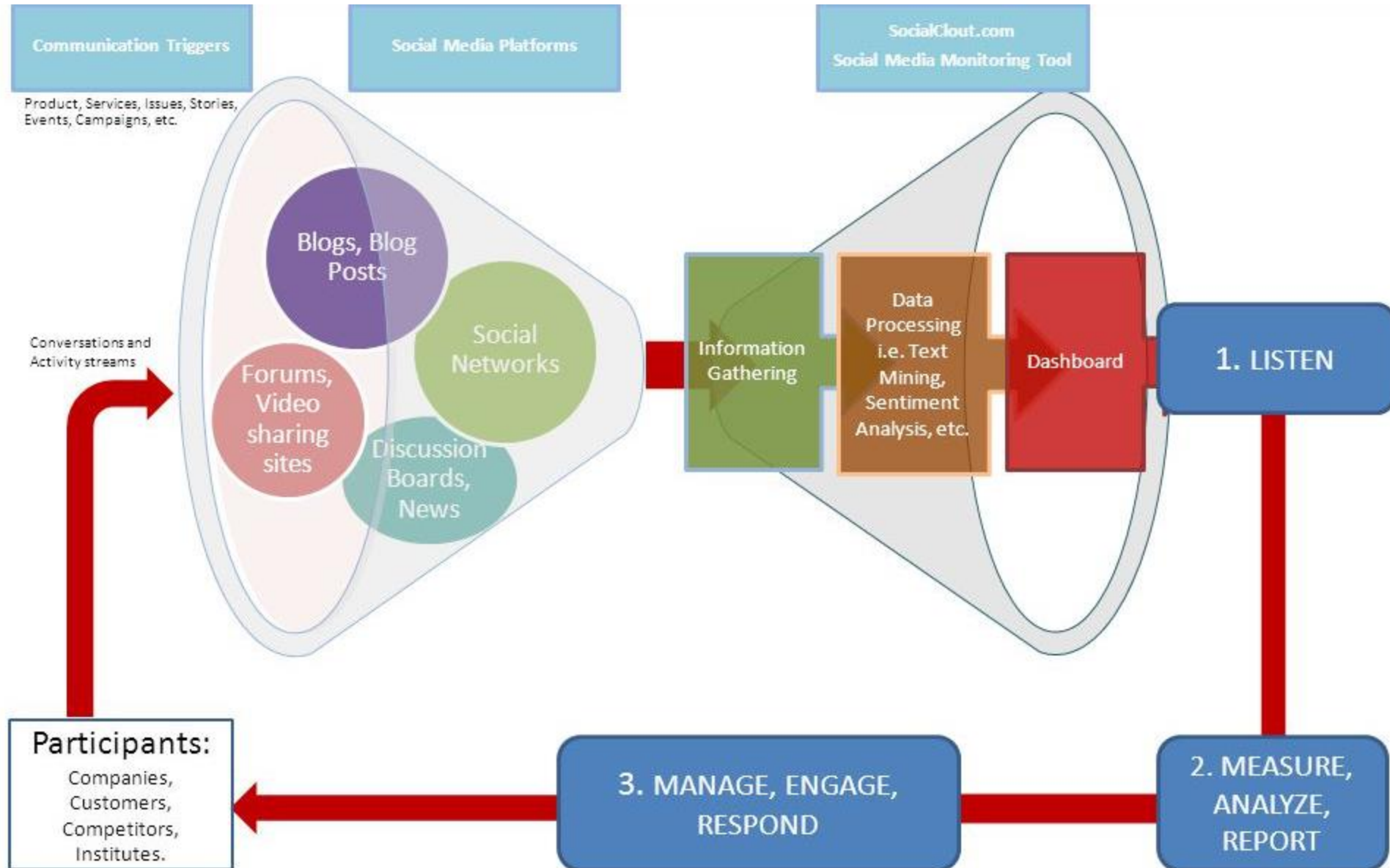
Community detection methods identify groups of actors that are more densely connected among each other than with the rest of the network.



OSINT Framework



Social Media Monitoring



Social Media Listening



SCOPE

Google Alerts Periodic check-ins on social channels	Monitor 'owned' social embassies, Monitor social for 'bad' news	Listen to brand conversations Follow competitors & industry trends	Listen and engage with a purpose Enterprise listening strategy	Insights to inform or recalibrate marketing or business strategy
---	---	--	--	---

STANCE



DATA



TOOLS

FREE TOOLS




PAID TOOLS




MULTIPLE TOOLS


CYBER SAFETY CHECKLIST




Back up online and offline files regularly and securely



Strengthen your home network




Use strong passwords




Keep your software updated



Manage social media profiles



Check privacy and security settings



Avoid opening and delete suspicious emails or attachments



INTERPOL

BE VIGILANT . BE SKEPTICAL . BE SAFE

How to Report Cyber Crime

भारत सरकार
GOVERNMENT OF INDIA

गृह मंत्रालय
MINISTRY OF HOME AFFAIRS

www.cybercrime.gov.in

Language 



राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
National Cyber Crime Reporting Portal

75
आज़ादी का
अमृत महोत्सव



Resources Section"



[REPORT WOMEN/CHILD RELATED CRIME +](#)

[REPORT OTHER CYBER CRIME](#)

[TRACK YOUR COMPLAINT](#)

[CYBER VOLUNTEERS +](#)

[RESOURCES +](#)

[CONTACT US](#)

[HELPLINE](#)



HELPLINE NUMBER



1930

If you are a victim of
Financial Cyber Fraud
Dial Helpline Number 1930



STAYING SAFE ON
**SOCIAL
MEDIA**





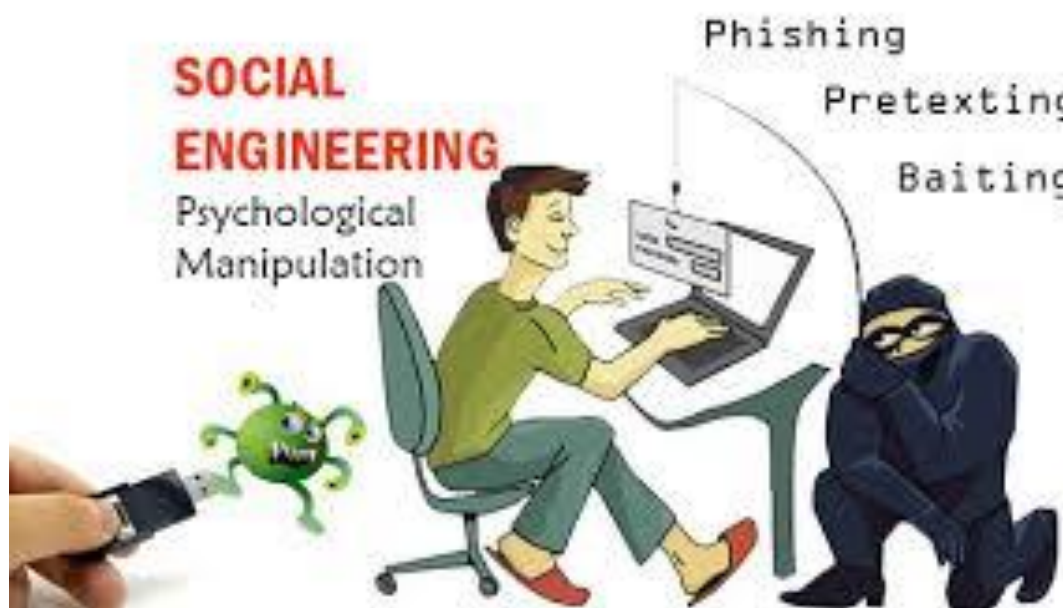
**SOCIAL
ENGINEERING**

Psychological
Manipulation

Phishing

Pretexting

Baiting



Advantages of e-Governance



Cybersecurity Threats



**Vulnerabilities
in the source
code**



**Misconfigured
system
components**



**Trust
configurations**



**Weak
credentialing
practices**



**Lack of
strong
encryption**



**Insider
threat**



**Psychological
vulnerability**



**Inadequate
authentication**



**Injection
flaws**



**Sensitive
data exposure**



**Insufficient
monitoring
and logs**

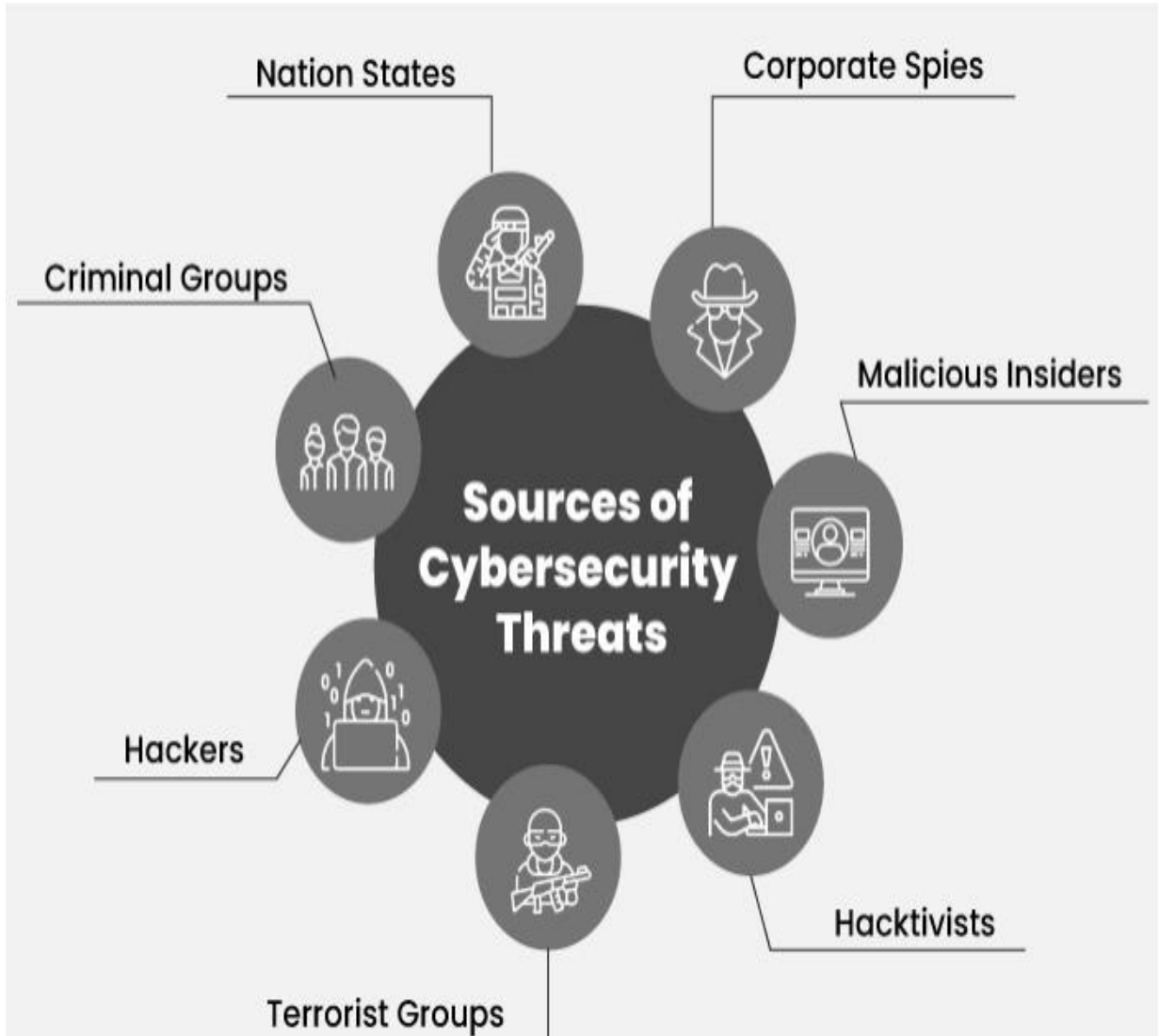


**Shared
tenancy
vulnerabilities**

OWASP Top 10 Vulnerabilities

2021 OWASP Top 10

- A01 Broken Access Control
- A02 Cryptographic Failures
- A03 Injection
- A04 Insecure Design
- A05 Security Misconfiguration
- A06 Vulnerable and Outdated Components
- A07 Identification and Authentication Failures
- A08 Software and Data Integrity Failures
- A09 Security Logging and Monitoring Failures
- A10 Server-Side Request Forgery (SSRF)



BEST WAYS TO IDENTIFY A SECURITY VULNERABILITY

- 01 Run a network audit


- 02 Analyze system log data


- 03 Use a penetration tester or white-hat hacker


- 04 Leverage a threat intelligence database


- 05 Simulate a social engineering attack


- 06 Use process mining to detect hidden flaws


- 07 Review the source code


- 08 Audit the IT supply chain


- 09 Automate the security testing process


- 10 Document the hardware landscape



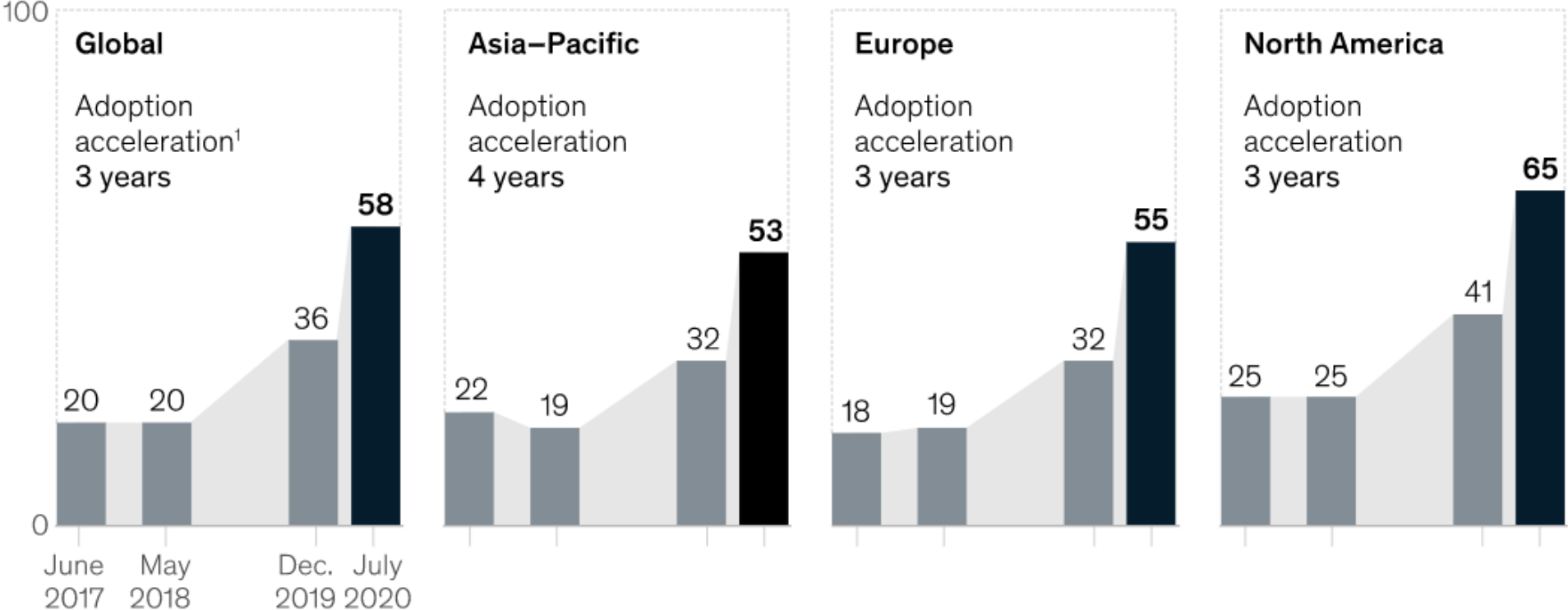


Sustainable Digitalisation

Digitization Adoption Rate

Average share of customer interactions that are digital, %

■ Precrisis ■ COVID-19 crisis





Understanding Cyber Crime

RECENT DATA BREACHES

2.5 mn



Airtel: Name, DoB, phone numbers, address, Aadhaar. Up for sale for bitcoins worth \$3,500

3.5 mn



MobiKwik: KYC info

20.0 mn

BigBasket: Personal information, address, PIN, IP addresses, etc for sale for \$40,000

22.0 mn

Unacademy: User name, password, and email

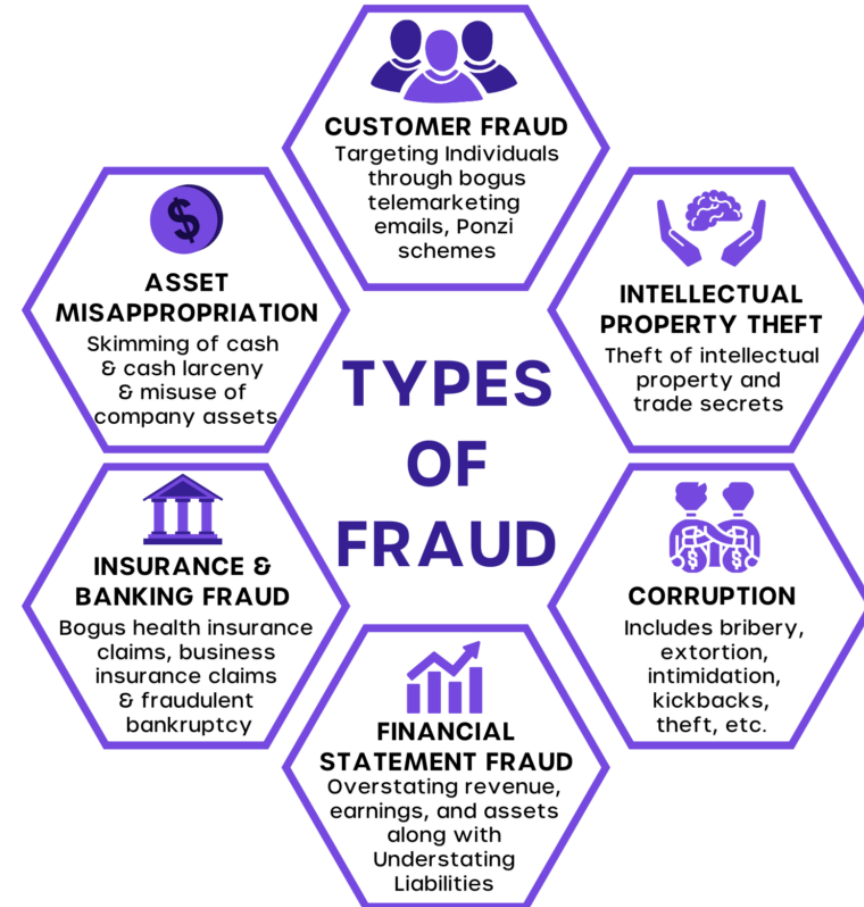
35.0 mn

Juspay: Masked card data & card fingerprint data was for sale for \$5,000
Bitcoins

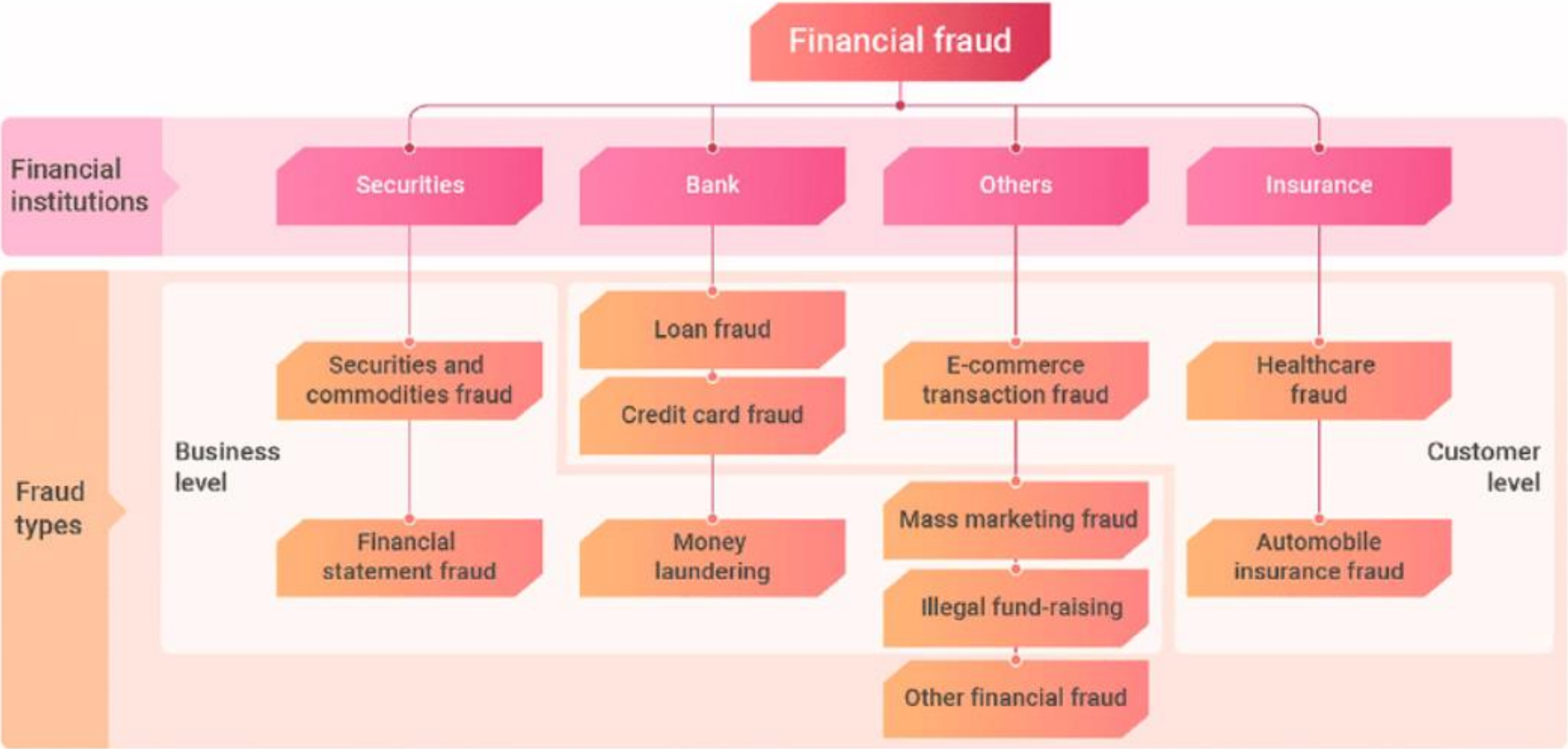
Source: News reports



Fraud Types



Fraud Classification



Banking Frauds



Cybercrime stats 2022

More than

90%

of **small and midsize enterprises** reported a cyber-attack that had a severe impact on their business.

By 2023, the **DDoS attack number** will rise to:

15.4 million

IOT gadgets get around:

52k

attack every month

Key Challenges in detecting Financial Fraud

Extremely high false positives



Fraud Detection Methods



LET'S DISCUSS



HUNTMETRICS

ayub@huntmetrics.tech

+91 900 040 4422