Microsoft

Cybersecurity and Cybercrime in the Digital Age

Piotr Marczuk, Corporate Affairs Director, Microsoft CEE

Evolving Threat Landscape

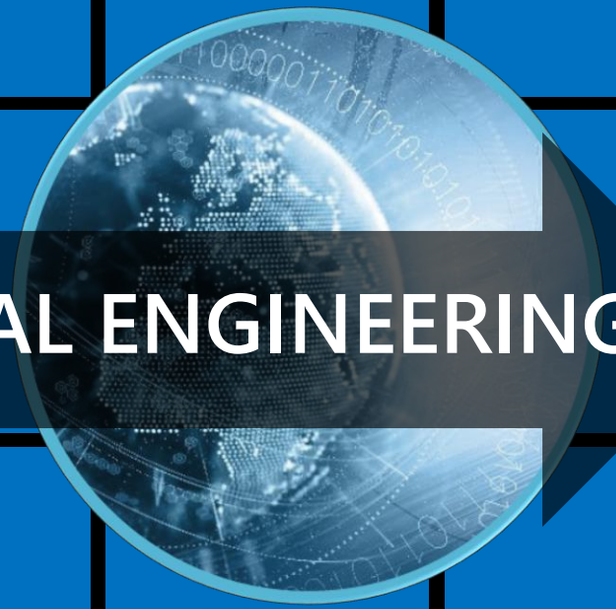
- **500k new malware** are created and spread every day
- **90% cyberattacks** begin with a phishing email
- **81% of breaches** involve weak or stolen passwords
- **87% of senior managers** admit to have accidentally leaked business data
- **99 days in average** from intrusion to detection
- **$150M estimated** cost per breach **by 2020**
- **$8 trillion** estimated cost of cybercrime to global economy **by 2022**
- **Emerge of AI and ML** is changing the game in cybersecurity

THE LEVEL OF SOPHISTICATION IS INCREASING

Hacking as a hobby

Hacking for financial gain

Nation-state attacks

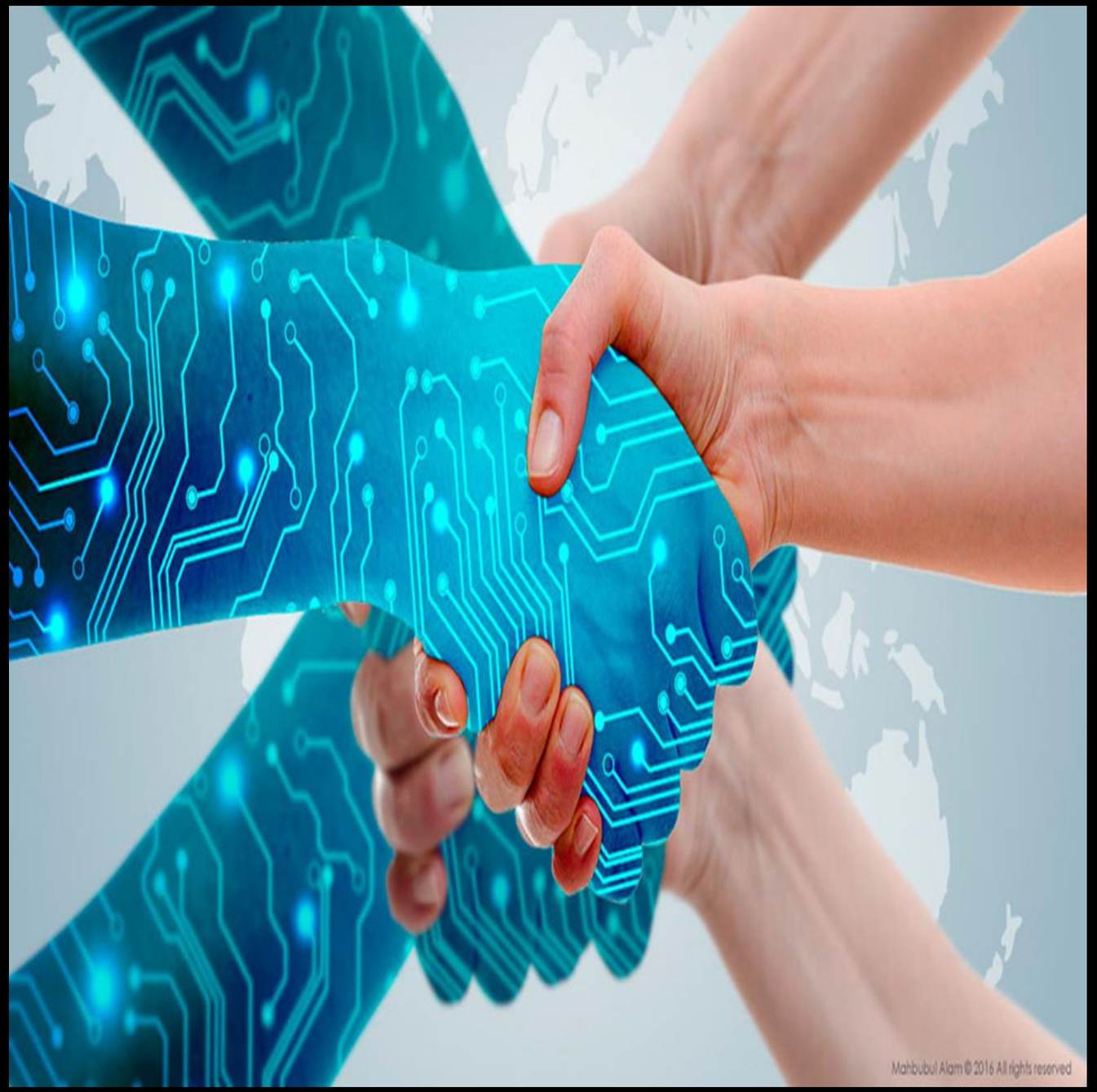


SOCIAL ENGINEERING

"**Security is an arms race**, and the security of machine learning and pattern recognition systems is not an exception"

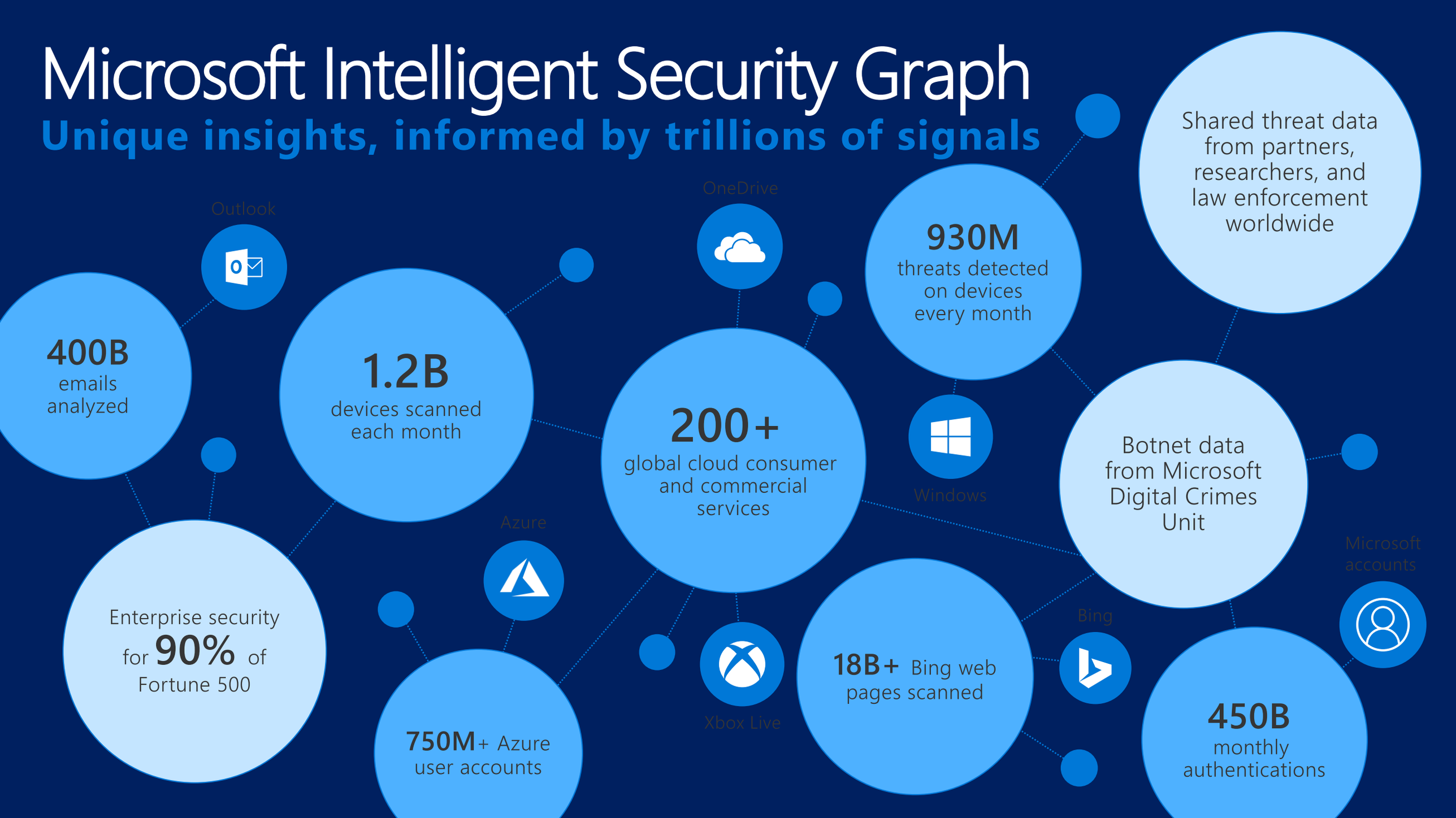
-- Battista Biggio, University of Cagliari

- Use of AI **requires effective methods to detect fraudulent behavior** and protect people from cyberattacks.
- At the same time, AI **plays an important role in developing new effective security** methods.

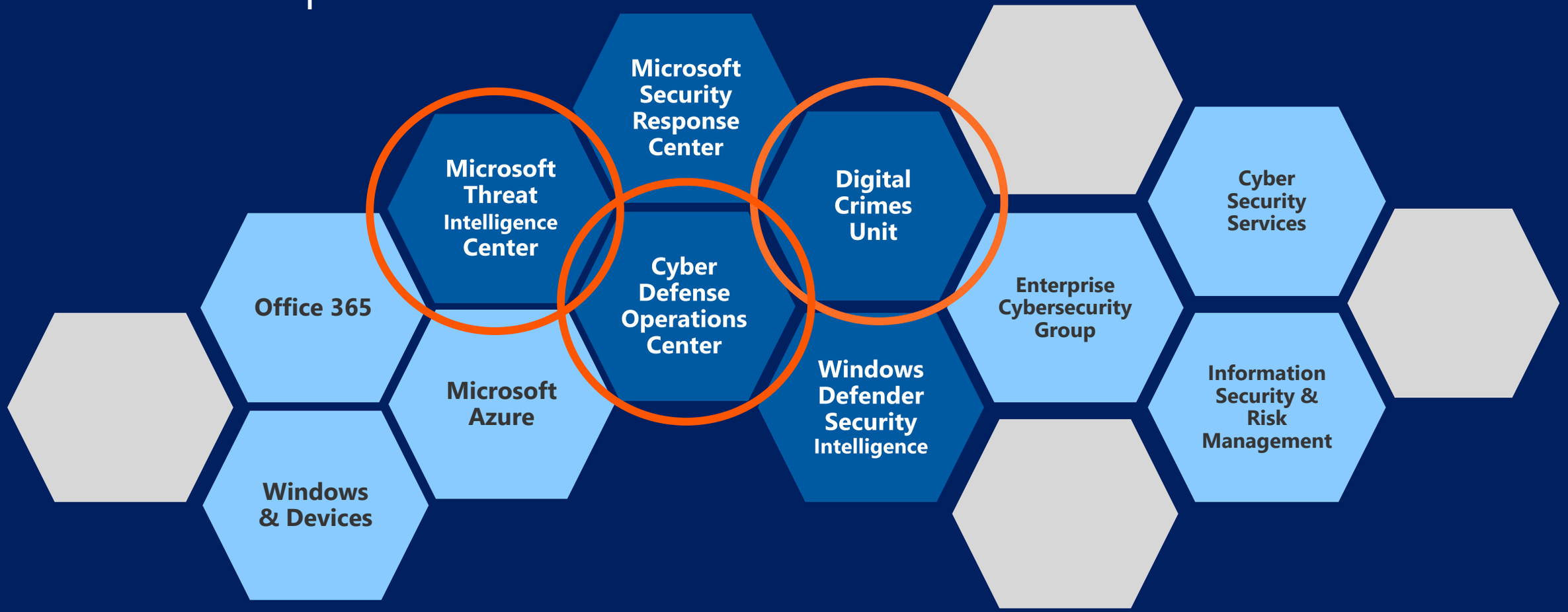


Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals

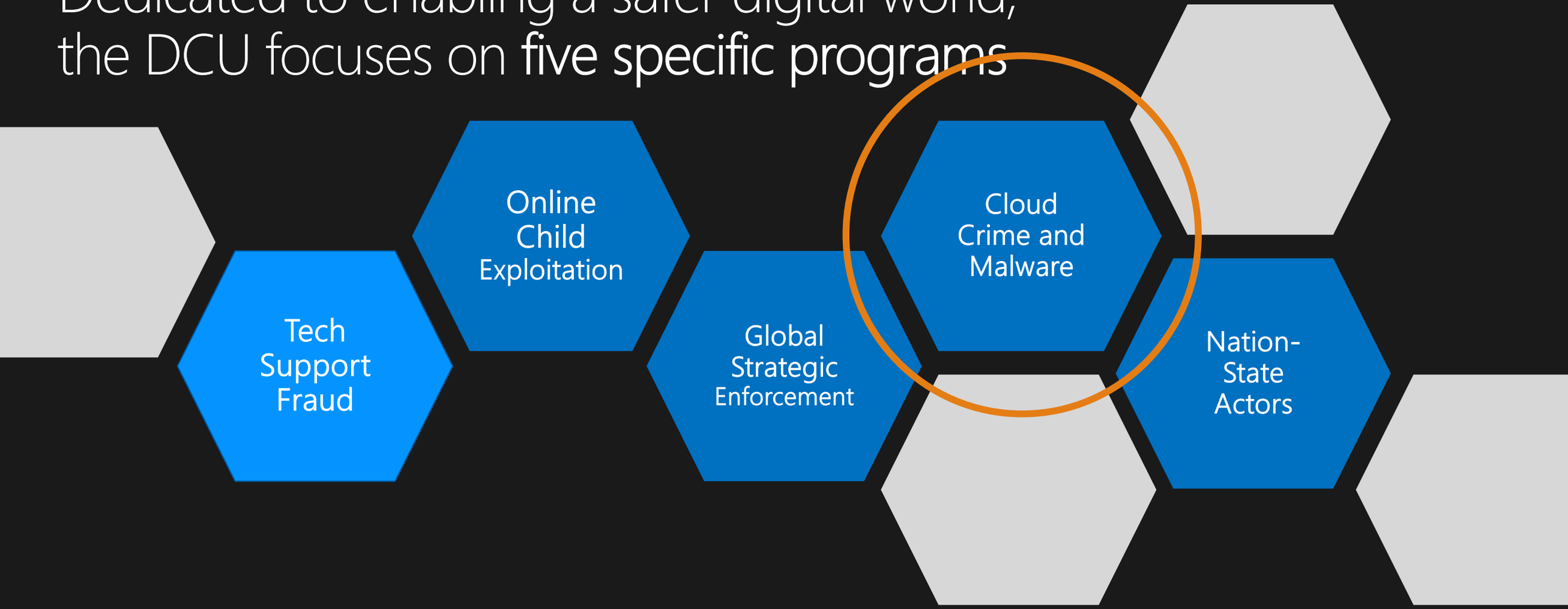


Working Together – **Coordinated** Response



DCU Programs

Dedicated to enabling a safer digital world,
the DCU focuses on **five specific programs**



Digital Crimes Unit

Leading the fight against cybercrime

Protecting people, organizations and our cloud through **global disruptions** and **enforcement actions** against cybercriminals

- Investigations, forensics and analytics
- Machine learning, AI and data visualization
- Public and private partnerships
- Creative legal strategies


CANADA
RUSSIA
KAZAKHSTAN
MONGOLIA
CHINA
BRAZIL
AUSTRALIA
Pacific Ocean
Atlantic Ocean
Indian Ocean
Labrador Sea
Hudson Bay
Gulf of Alaska
Sea of Okhotsk
Yellow Sea
East China Sea
Philippine Sea
South China Sea
Bay of Bengal
Arabian Sea
Gulf of Guinea
Java Sea
Banda Sea
Coral Sea
Tasman Sea
Caribbean Sea
Norwegian Sea
ICELAND
SWEDEN
FINLAND
NORWAY
MEXICO
COLOMBIA
PERU
CHILE
ARGENTINA
MALI
ETHIOPIA
SOMALIA
KENYA
GABON
CONGO (DRC)
NAMIBIA
BOTSWANA
SOUTH AFRICA
MADAGASCAR
INDONESIA
PHILIPPINES
PAPUA NEW GUINEA
JAPAN

Botnet Takedowns and Malware Disruption Operations

OPERATION Conficker

Feb 2010
Microsoft-lead model of industry-wide efforts to counter the threat

Botnet Worm sending SPAM and attempting to steal confidential data and passwords

OPERATION Waledac

Feb 2010
First MS takedown operation, proving the model of industry-led efforts
Disconnected70,000-90,000 infected devices from the botnet

Botnet Worm sending SPAM

OPERATION Rustock

March 2011
Supported by stakeholders across industry sectors
Involved US and Dutch law enforcement, and CN-CERT

SPAM, in average 192 spam messages per compromised machine per minute

OPERATION Kelihos

Sep 2011
Partnership between Microsoft and security software vendors
First operation with named defendant

SPAM, Bitcoin Mining, DDoS attacks

OPERATION Zeus

March 2012
Cross-sector partnership with financial services
Focused on disruption because of technical complexity

Identity Theft / Financial Fraud

OPERATION Nitol

Sep 2012
Nitol was introduced in the supply chain relied on by Chinese consumers settled with operator of malicious domain

Malware Spreading, DDoS attacks

OPERATION Bamital

Feb 2013
Bamital hijacked people's search results, took victims to dangerous sites
Takedown in collaboration with Symantec, proactive notification and cleanup process

Advertising Click Fraud

OPERATION Citadel

June 2013
Citadel committed online financial fraud responsible for more than $500Min losses
Coordinated disruption with public-private sector

Identity Theft / Financial Fraud

OPERATION Sirefef

Dec 2013
ZeroAccess hijacked search results, taking victims to dangerous sites
It cost online advertisers upwards of $2.7 million each month

Advertising Click Fraud

OPERATION Game over Zeus

June 2014
GameoverZeus (GOZ) was a banking Trojan

Worked in partnership with LE providing Technical Remediation

Identity Theft / Financial Fraud

OPERATION Bladabindi & Jenxcus

June 2014
Malware using Dynamic DNS for command. It involved password and identity theft, webcam, etc.
Over 200 different types of malware impacted.

Identity Theft / Financial Fraud / Privacy Invasion

OPERATION Caphaw

July 2014
Caphaw was focused on online financial fraud responsible for more than $250M in losses

Coordinated disruption with public-private sector

Identity Theft / Financial Fraud

OPERATION Ramnit

Feb 2015
Malware stealing credential information from banking websites. Configured to hide itself.

Credential Information Theft/Disabling Security Defenses

OPERATION Simda

April 2015
Theft of personal information, including banking passwords, as well as installing and spreading other malicious malware.

Theft personal data/Install and spread other malware

OPERATION Dorkbot

December 2015
Used for Cybercriminal activities such as credential harvesting for financial fraud
DDoS attacks and the downloading of malicious payloads.

Financial Fraud, DDoS Attacks

OPERATION Avalanche

November 2017
Int'l criminal syndicate involved in phishing attacks, online bank fraud, and ransomware. Also refers to the network of systems used to carry out the activity. Initial takedown global law enforcement occurred on 30 November 2016.

Criminal Syndicate

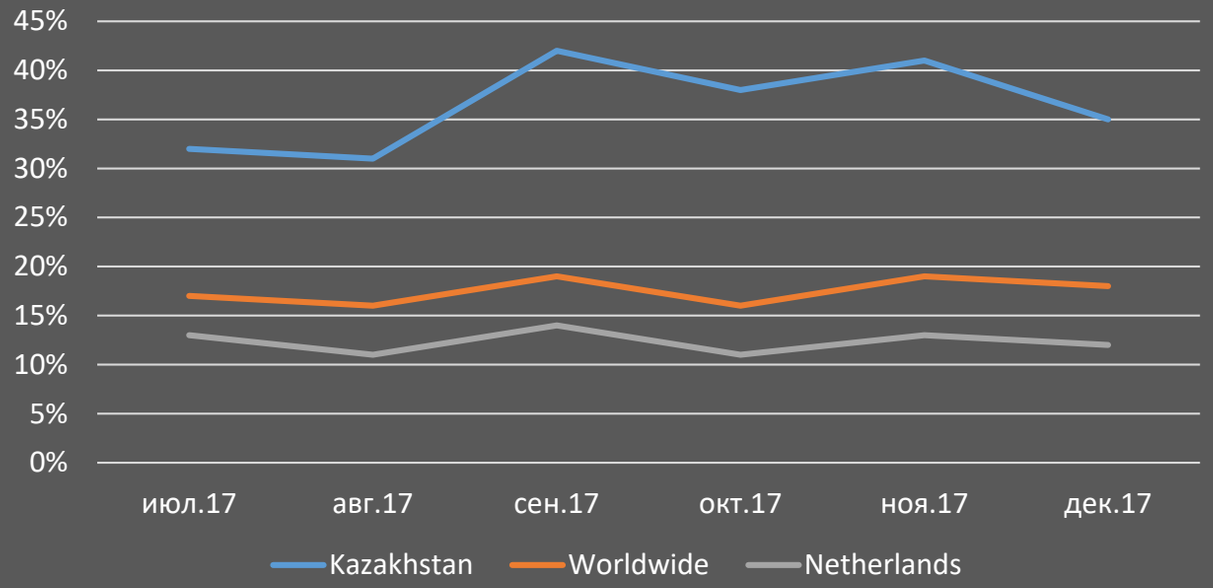
OPERATION Gamarue

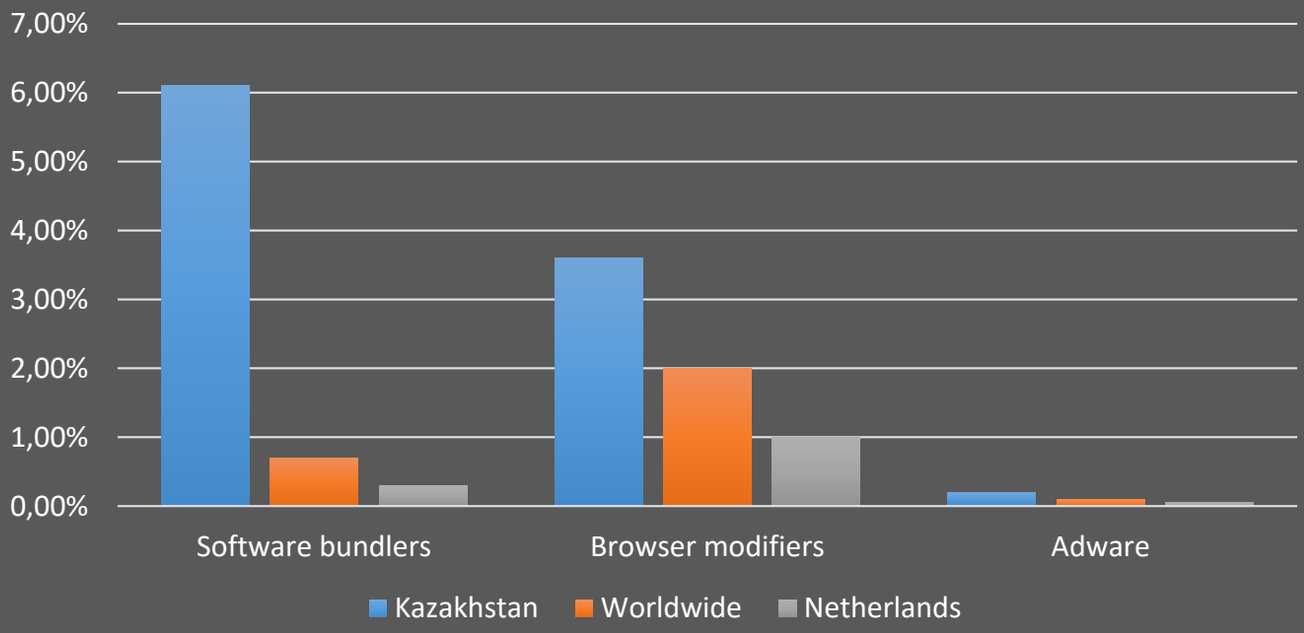
November 2017
Sold as a Crime kit, AKA Andromeda bot, first seen in Apr 2012. Distributed at least 80 different malware families.
Disruption started Dec 2015 involving Windows Defender team, DCU and partnered with ESET, global LE agencies, and private industry partners.

Malware Spreading Botnet


Threats 30 - Days
Avalanche
B106
Bamital
Caphaw
Citadel
Conficker
Dorkbot
Gamarue
Gameover Zeus
Ramnit
Simda
Sirefef
Waledac
Zbot
SWEDEN
NORWAY
FINLAND
Oslo
Stockholm
Helsinki
Tallinn
ESTONIA
Riga
LATVIA
Moscow
North Sea
DENMARK
Copenhagen
UNITED KINGDOM
Dublin
Baile Atha Cliath
IRELAND
London
Celtic Sea
NETHERLANDS
Amsterdam
Hamburg
Bremen
Hannover
Berlin
Poznań
Warsaw
POLAND
Dortmund
Düsseldorf
GERMANY
Wrocław
BELGIUM
Frankfurt
Prague
Kraków
CZECH REPUBLIC
Saint Peter Port
Saint Helier
LUXEMBOURG
Paris
Strasbourg
Stuttgart
Munich
Vienna
Bratislava
SLOVAKIA
Budapest
HUNGARY
Kyiv
UKRAINE
MOLDOVA
FRANCE
SWITZERLAND
AUSTRIA
SLOVENIA
ROMANIA
Bucharest
Black Sea
Bay of Biscay
Toulouse
Marseille
MONACO
Turin
Milan
Genoa
CROATIA
Belgrade
BOSNIA AND HERZEGOVINA
SERBIA
BULGARIA
ANDORRA
Barcelona
ITALY
Adriatic Sea
Rome
Naples
Sea of Sardinia
Tyrrhenian Sea
Ionian Sea
Palermo
Cagliari
Ankara
TURKEY
Yerevan
Lisbon
PORTUGAL
SPAIN
Valencia
Seville
Palma
GREECE
Athens
Patras
Nicosia
SYRIA
Baghdad
LEBANON
Damascus
JORDAN
ISRAEL
Algiers
Oran
Bejaia
Tunis
Rabat
Oujda
Fez
MOROCCO
Marrakesh
Agadir
TUNISIA
MALTA
Mediterranean Sea
Tripoli
Benghazi
Cairo
EGYPT
SAUDI ARABIA
ALGERIA
LIBYA
WESTERN SAHARA
Nouakchott
MAURITANIA
Dakar
SUDAN
IRAN
IRAQ

Malware and NG soft rate trends in **Kazakhstan** & **Netherlands**





Challanges to Kazakh companies & startups in building digital economy and adopting AI

Cybersecurity risks

Unclarity and misinterpretation of data protection regulations

Data localization policy („Digitization law")

Digital Policy Recommendations

Strenghten collaboration between Government and IT Industry to combat NG software and improve cybersecurity with reasonable and affordable cost – hybrid model recommended

Create a working group between Government, Business & IT Industry to identify and amend data management policies (build on EU example)

Develop Government guidelines on the use of Cloud with appriopiate security safeguards to accelerate Digital Kazakhstan and Artificial Intelligence development and adoption


TRUST

Microsoft

Thank You

find me on linkedin

www.linkedin.com/in/piotrmarczuk