PEACE AND STABILITY IN CYBERSPACE

FACTSHEET

With its potential to **galvanise growth** and **increase prosperity**, the digital economy is now high on the global agenda. Internet-enabled platforms, data-driven innovation and digital applications are **changing the workings of all sectors**, including transportation, health, education and agriculture.

Yet, these benefits are not always enjoyed equally around the globe – not least due to the digital divide but also to cybercrime and malicious activities undertaken in cyberspace by state and non-state actors.

DATA BREACHES

Social institutions, organisations and businesses of all sizes have become increasingly reliant on digital data. Breaches exposing sensitive personally identifiable information that would otherwise be kept confidential, such as health or financial records, have become larger in scope and more damaging in impact

CYBER CONFLICT

Nation states and state-sponsored hacker groups continue to leverage sophisticated cyber-capabilities to achieve geopolitical aims, influence international politics, and interfere with electoral systems and governmental functions, thereby increasing the risk of misinterpretation and unwanted escalation into conflict

HACKTIVISM

Cyberspace is increasingly used by groups of hackers who target governmental actors, media outlets and political regimes through the defacing of websites, DDoS attacks and confidential information leaks in order to convey political and social messages

CYBER ESPIONAGE

Cyber espionage continues to present a pervasive threat to EU security and its competitive advantage. Intellectual property and sensitive military and civilian technology is being stolen by nation states, as well as organised cybercrime and proxy groups so as to gain economic advantages in strategic industries

Stuxnet
Iran. Jun 2012
Physical damage to centrifuges used in the uranium enrichment process at the Natanz nuclear facility

67%
increase in **security breaches** in the last five years

Yahoo!
Aug 2013
3,000,000,000 accounts compromised

Sony Pictures
US. Nov 2014
Significant business operations disruption, release of terabytes of proprietary data and sensitive information

APT1 (Unit 61398)
2013
141 companies in **15 countries** spanning 20 major industries compromised

BlackEnergy
Ukraine. Dec 2015
Loss of power for several hours

CyberBerkut
Germany. Jan 2015
DDoS attacks against government websites

Democratic National Committee
US. Jun 2016
Interference in 2016 US presidential election. Release of confidential and campaign emails and files

#OpSingleGateway
Thailand. Oct 2015
DDoS attacks against government websites

$13m
average cost of **cyber attacks on companies** in 2019

WannaCry/NotPetya
Ukraine. May 2017
Disruption of public services

Anonymous-affiliated
US. Oct 2016
DDoS attack against DNS provider, disabling websites

APT28 (Fancy Bear)
2016
over **15 entities and organisations** in Europe and the Americas compromised

Equifax
US. Jul 2017
143,000,000 records lost

OlympicDestroyer
South Korea. Feb 2018
Paralysis of public sector infrastructure

Binary Guardians
Venezuela. Aug 2017
Defacing of over **40 government websites**

SinghHealth
Singapore. Jul 2018
1,500,000 medical records lost

APT10 (Cloud Hopper)
2017
42 companies in **12 countries**, spanning **20 major industries** compromised

Marriott Hotels
Nov 2018
383,000,000 records lost

Taoabdegan
Iran. May 2018
Hacking of Mahshad international airport system

Data: FireEye 2019; CrowdStrike 2018; Breach Level Index 2019; Council on Foreign Relations 2019

Conflict and malicious activities in cyberspace always come at a cost. These can be financial (loss of profit), political (loss of trust, over-regulation) or societal (curbs on fundamental freedoms) in nature. **Cyber diplomacy has become the main avenue for protecting the rules-based international order and imposing consequences on perpetrators of malicious cyber activities.**
A common and comprehensive EU approach to cyber diplomacy contributes to the mitigation of cybersecurity threats, conflict prevention and greater international stability through the use of diplomatic and legal instruments.

THE EUROPEAN UNION AS A CYBER PLAYER

THE EU SETS GOOD PRACTICES FOR STRENGTHENING CYBER RESILIENCE

> It strengthens its domestic resilience by **setting standards**, promoting **cooperation** among stakeholders and **building a culture of cybersecurity** across all sectors.

> It is one of the world's biggest donors in **cyber capacity-building** projects worldwide focused on developing national cybersecurity strategies, establishing CERTs and fighting cybercrime – all with respect for human rights and fundamental freedoms.

THE EU IS PROMOTES RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE

> It strongly advocates that **existing international law applies in cyberspace** and emphasises that respect for international law, in particular the UN Charter, is **essential to maintaining international peace and security**.

> It acknowledges that compliance with voluntary, non-binding **norms of responsible state behaviour in cyberspace** contributes to an **open, secure, stable, accessible and peaceful cyberspace**.

THE EU BUILDS TRUST TO REDUCE THE RISK OF MISPERCEPTION, ESCALATION AND CONFLICT

> It has actively supported the development of two sets of **confidence-building measures** adopted by the OSCE, as well as similar processes in Latin America and Asia Pacific.

CYBER DIPLOMACY TOOLBOX

> **Political statements** by high-level EU representatives

> **General or specific conclusions** by the Council of the European Union

> **Joint requests** for technical assistance to third countries

> **Diplomatic démarches** by EU delegations

> EU bilateral and multilateral topical and **political dialogues**

> **Restrictive measures**

> Other forms of **diplomatic pressure**

EXAMPLES OF CYBER NORMS PROMOTED BY THE EU

> **States must not** use proxies to commit **internationally wrongful acts** by using ICTs

> **States should seek** to ensure that their territory is not used by non-state actors to commit internationally wrongful acts

> **States should not** conduct or knowingly support ICT activities contrary to their obligations under international law

EU CYBER DIRECT
Supporting EU Cyber Diplomacy

This project is funded by the European Union.