Cyber Diplomacy Workshop

15th-16th April 2024

African Union Commission

Addis Ababa

Workshop page with:
- Draft Blueprint for Cyber Diplomacy in Africa
- AI Chatbot
- Slides
- Resources

https://www.diplomacy.edu/cyber-diplomacy-africa/
(pass: diplo)

Cybersecurity
and
cyber diplomacy

Part I
Risks

Case Studies

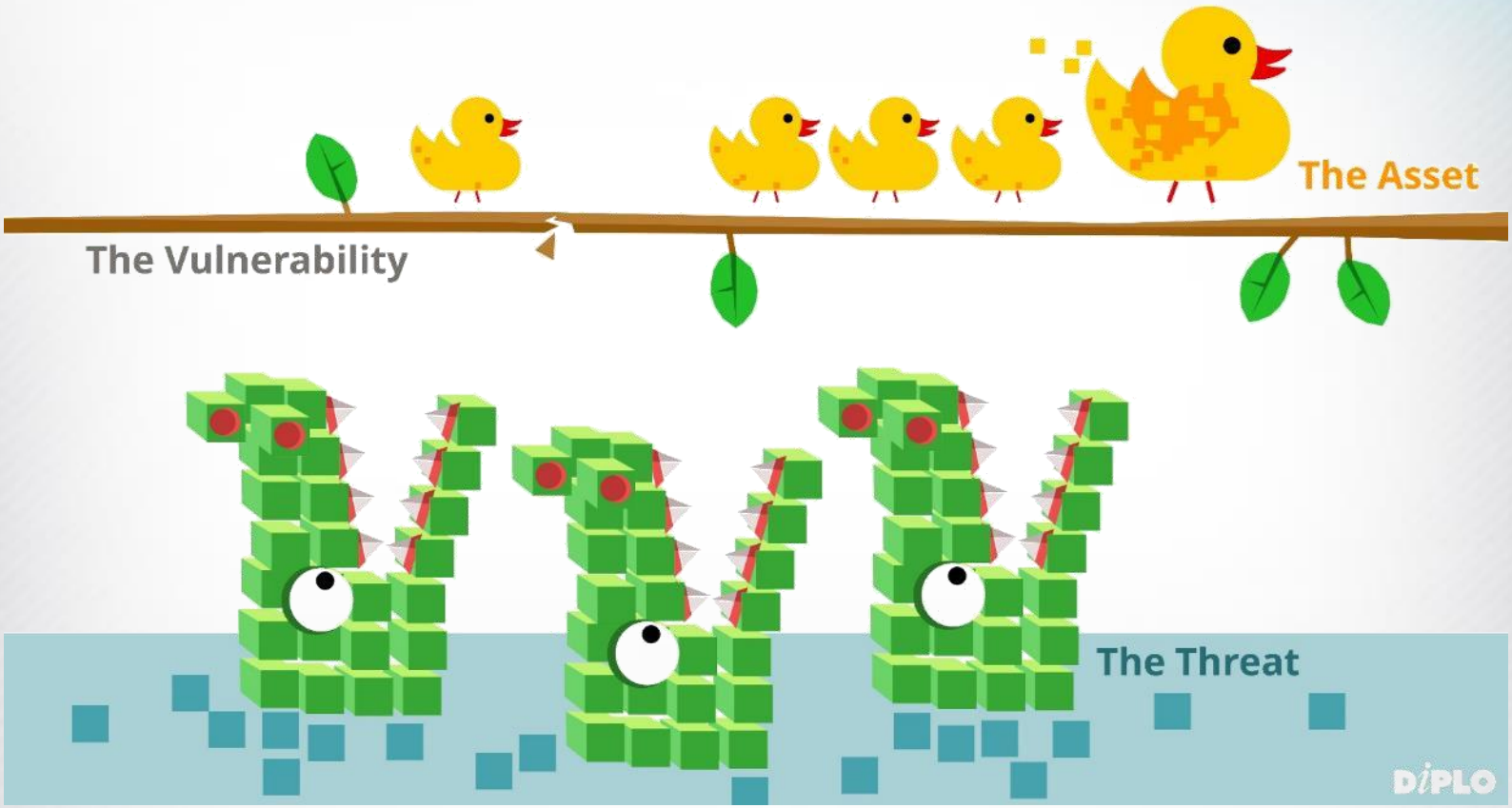

Ivano-Frankivsk Oblast, Ukraine, 23 December 2015,15:35

Woldwide, 15 May 2017, morning

Copenhagen, 27 June 2017, 8:15

Geopolitical Risks

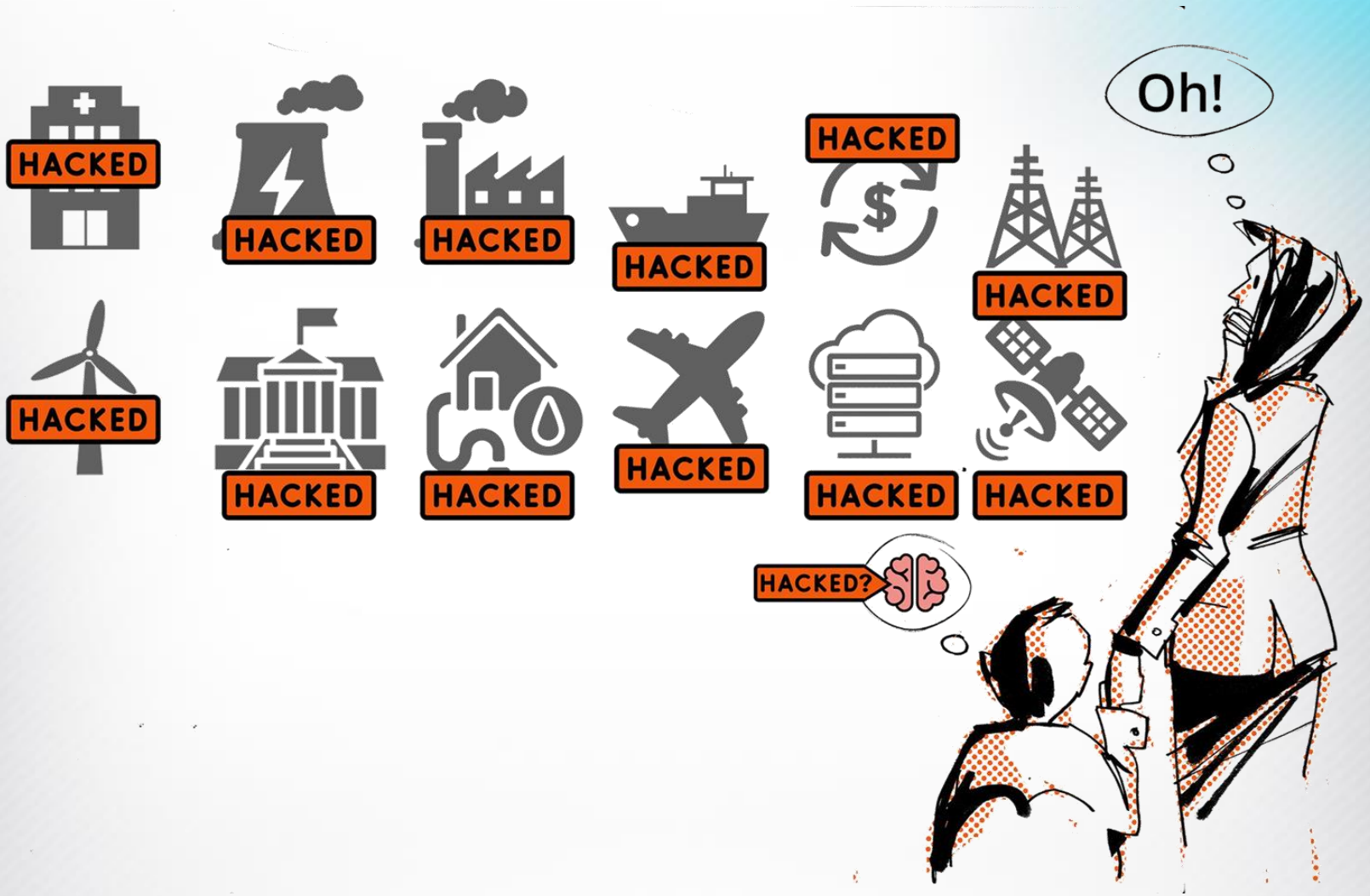
Risks



Risk = Assets x Threats x Vulnerabilities

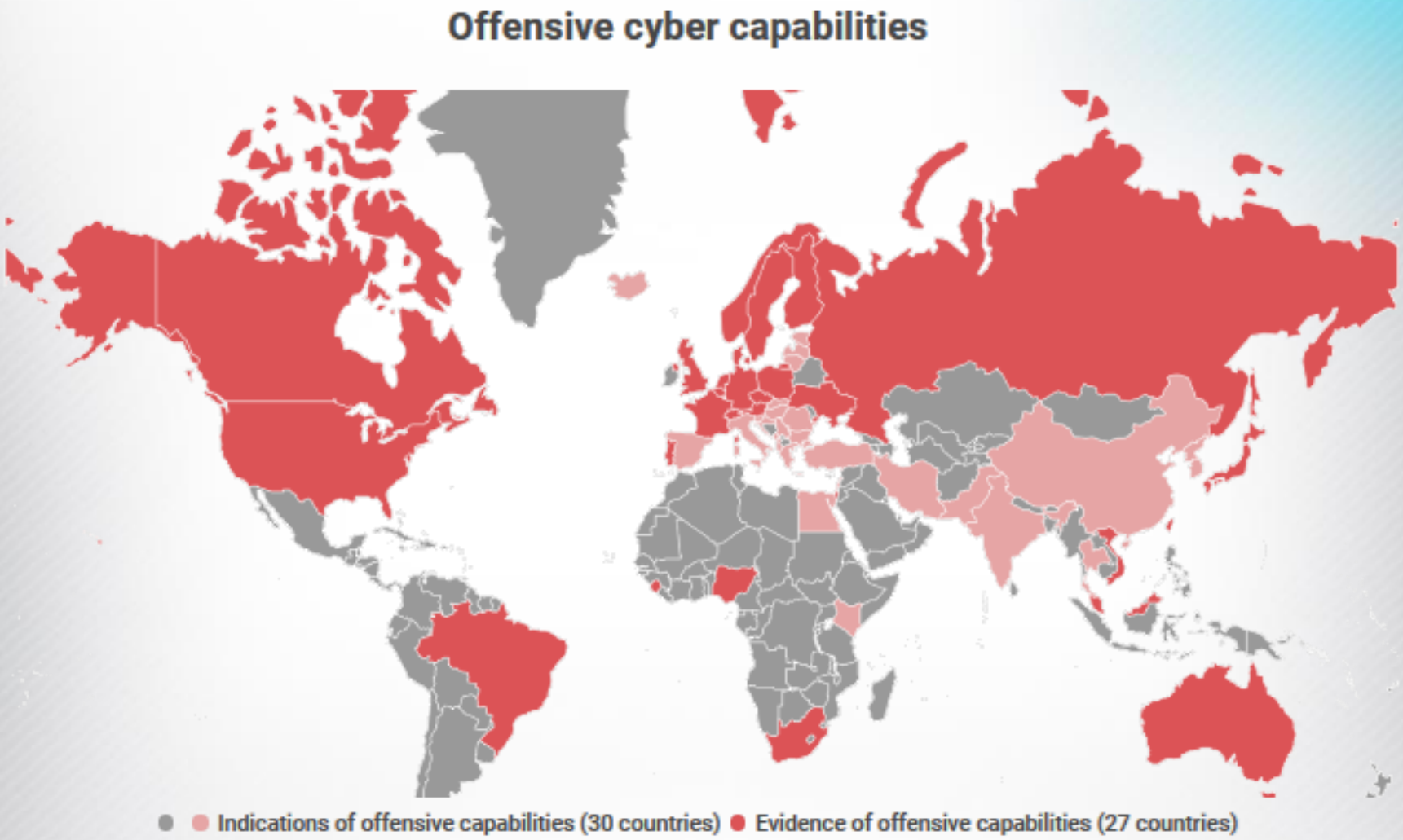
DiPLO
www.diplomacy.edu

Assets


HACKED
HACKED
HACKED
HACKED
HACKED
HACKED
HACKED
HACKED
HACKED
HACKED
HACKED
HACKED
Oh!
HACKED?

Whatever is **digitalized/connected** can be **hacked**.

Threats



Available at: https://dig.watch/topics/cyberconflict

DiPLO
www.diplomacy.edu

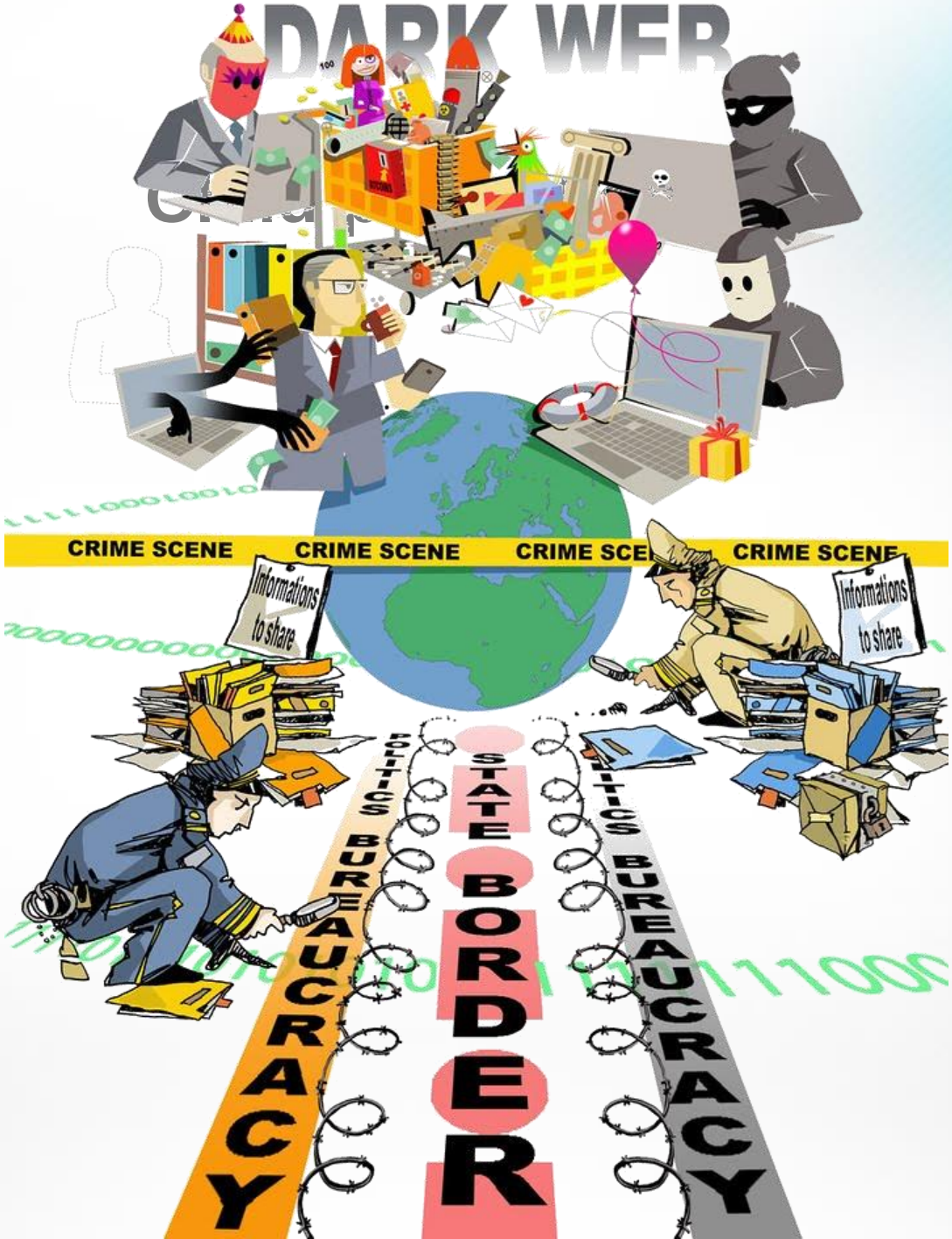
Cybersecurity Issues

DiPLO
www.diplomacy.edu

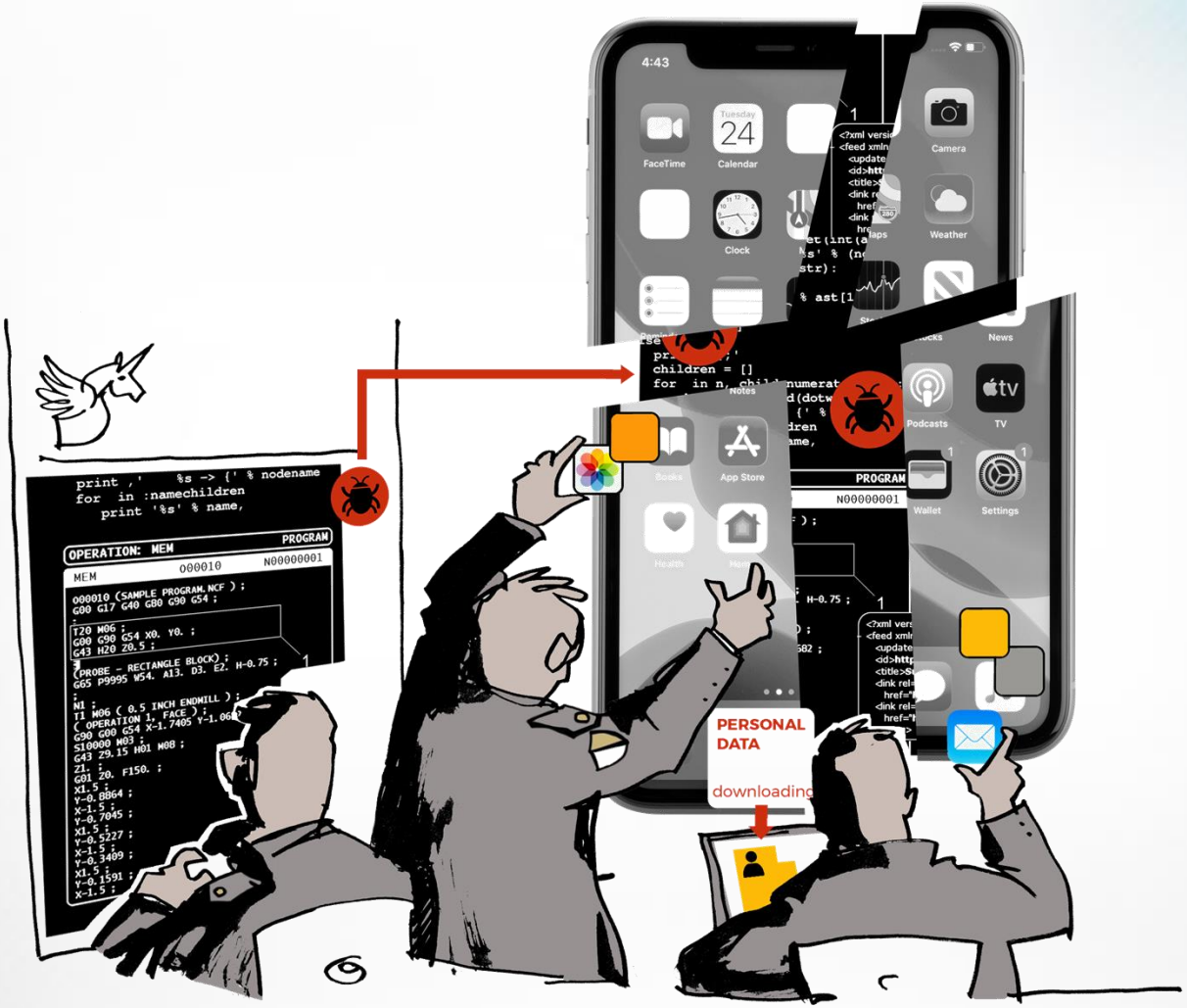
Cyber-warfare

Disinformation

Cybercrime



Cyber espionage and surveillance



DiPLO
www.diplomacy.edu

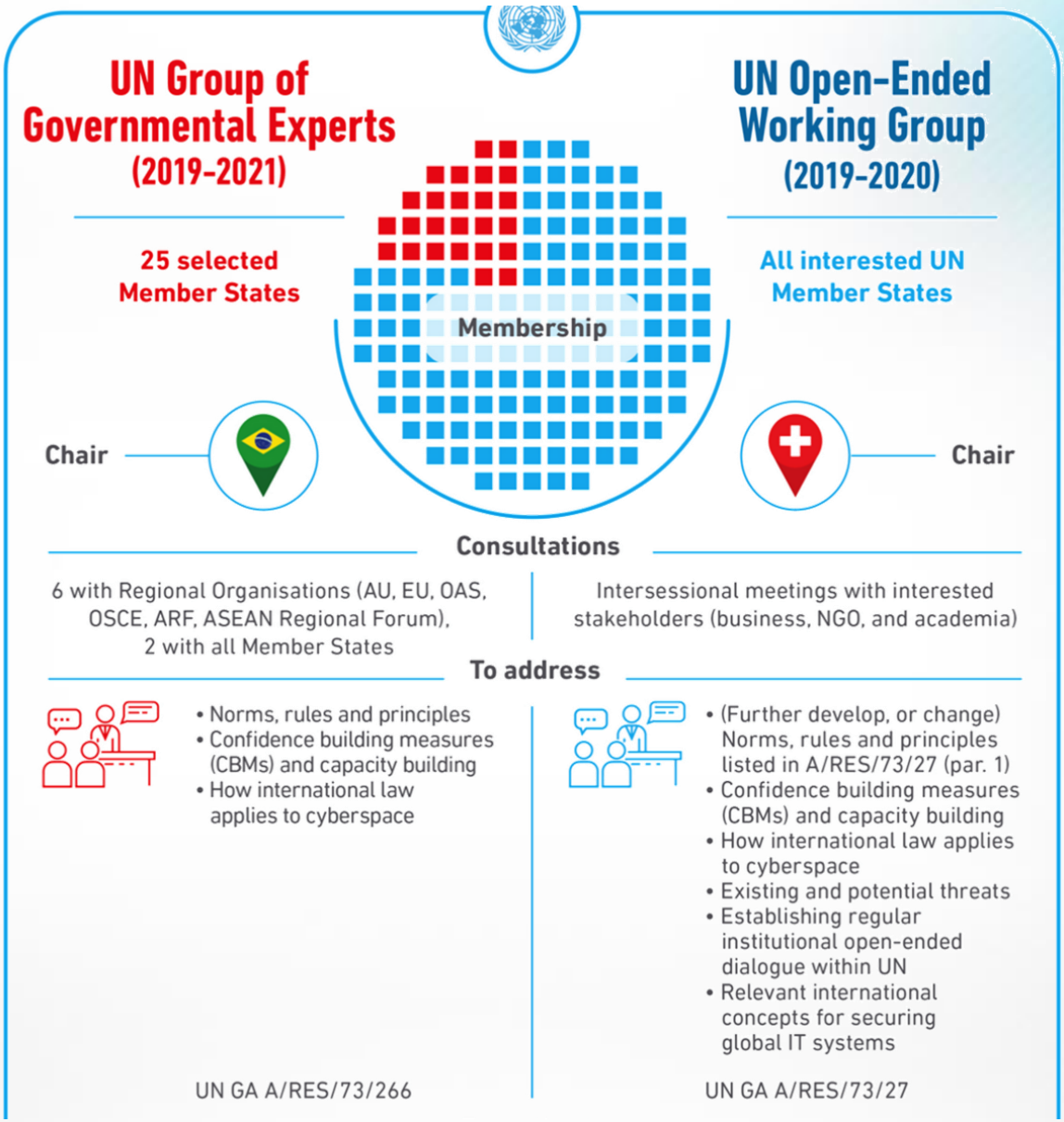
AI and cybersecurity: Autonomous Lethal Weapons

Watch: https://www.youtube.com/watch?v=LLQUDoT95Yg

DiPLO
www.diplomacy.edu

Part II
Framework

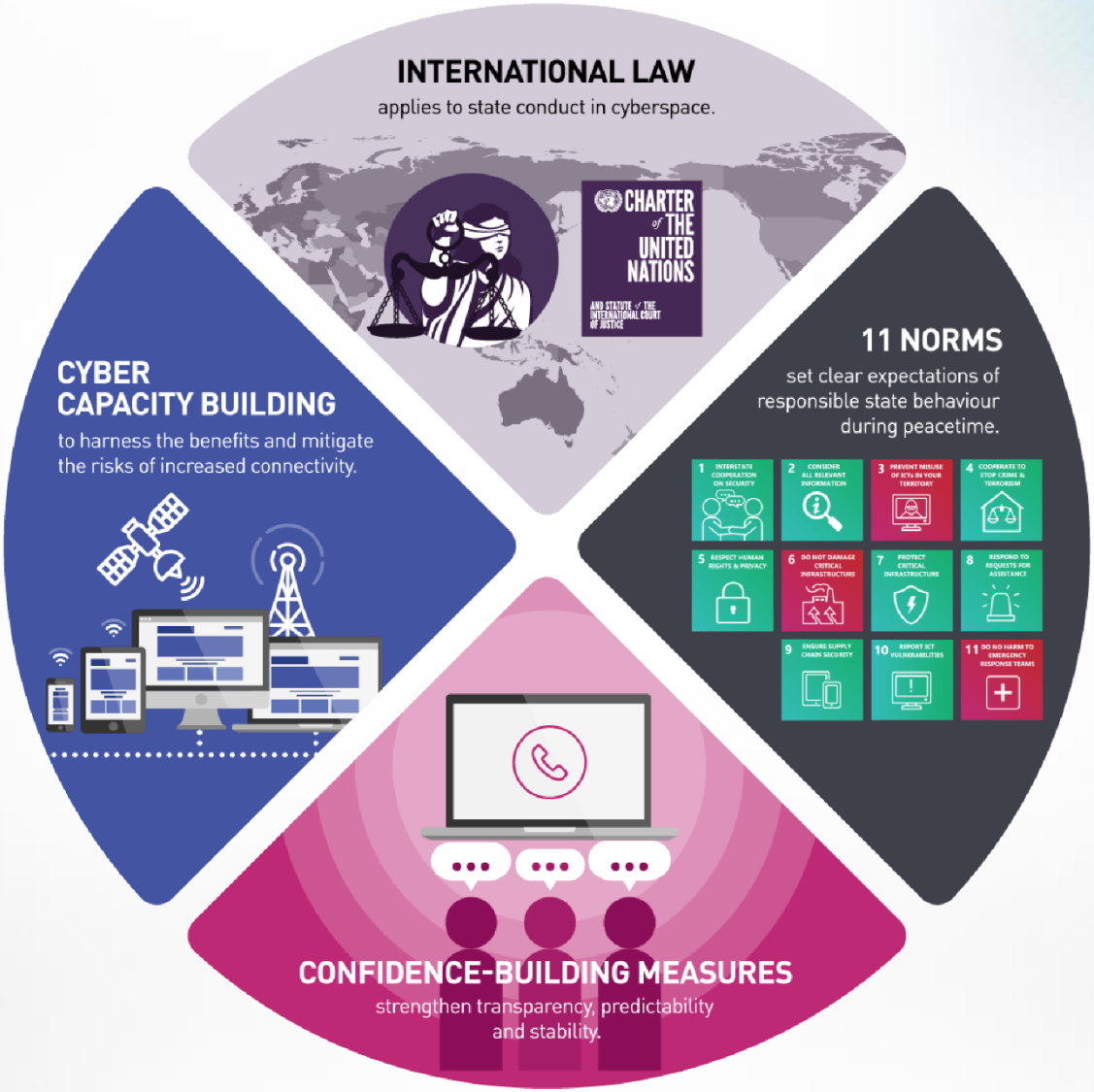
History



Source: https://dig.watch/ungge

DiPLO
www.diplomacy.edu

UN framework of responsible state behaviour in cyberspace

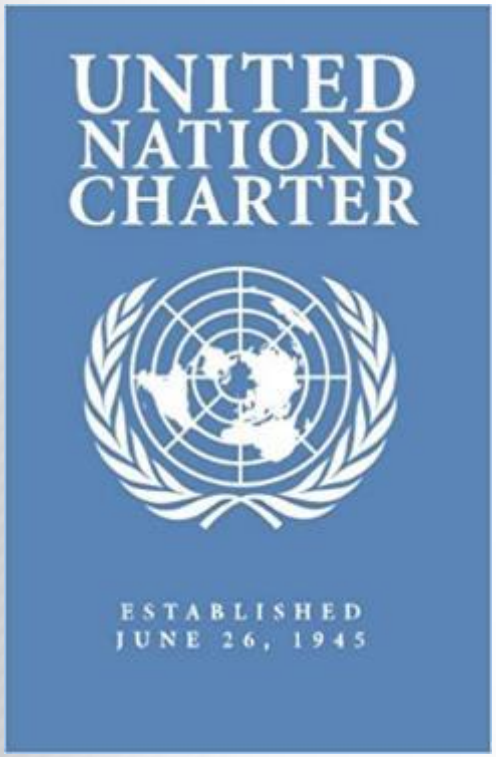


Source: ASPI

DiPLO
www.diplomacy.edu

Applicability of international law

Applicability of the international law to cyberspace



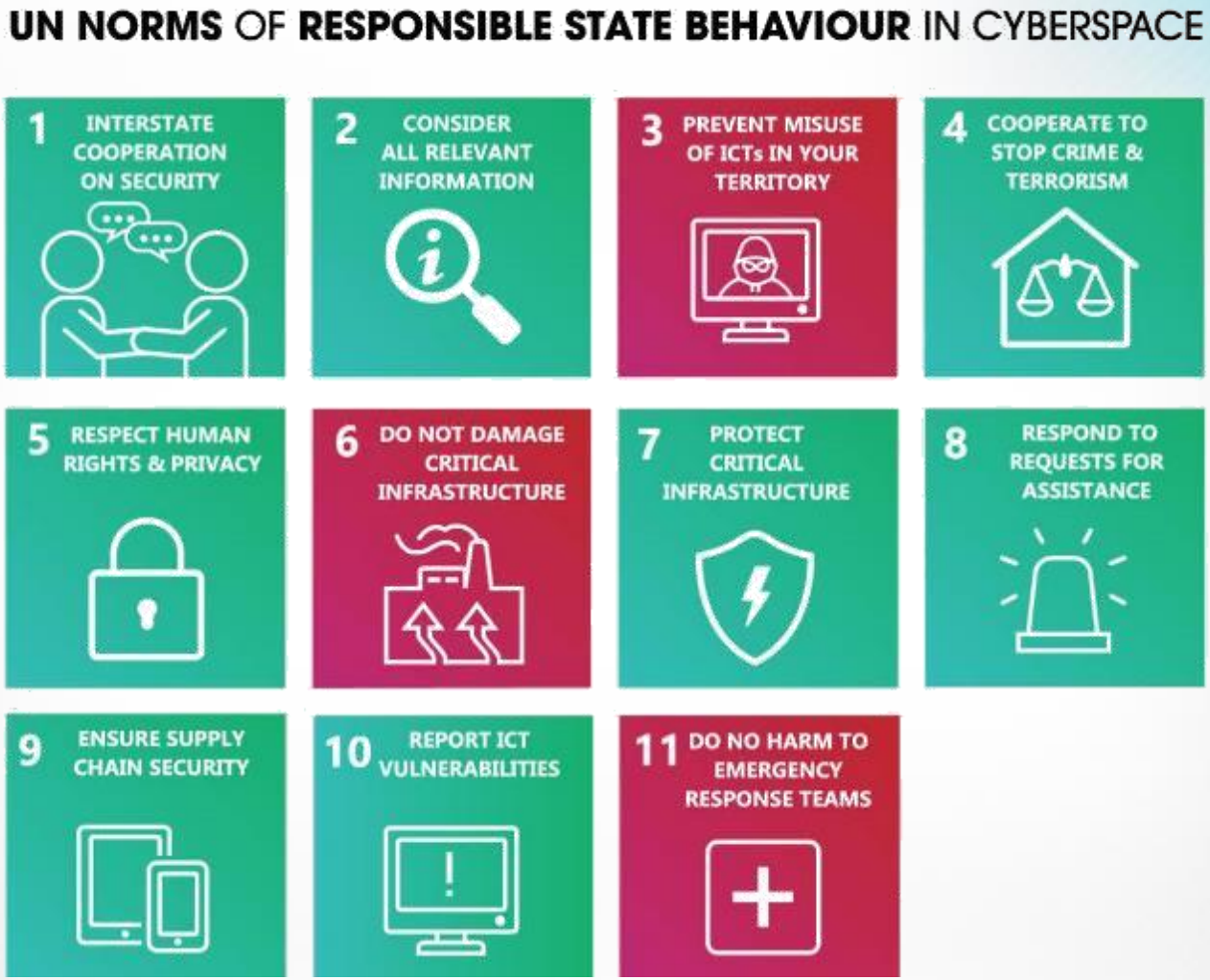
(How) Does the international law apply to cyberspace?

States reaffirmed that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment.

How does the international law apply to cyberspace?
What about human rights law and humanitarian law?
What are national positions on applicability of international law?

Cyber Norms

Cyber-norms



Source: ASPI

Limiting norms

- States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;
- States should not conduct or knowingly support ICT activity that intentionally damages critical infrastructure;
- States should take steps to ensure supply chain security, and should seek to prevent the proliferation of malicious ICT and the use of harmful hidden functions;
- States should not conduct or knowingly support activity to harm the information systems of another state's emergency response teams (CERT/CSIRTS) and should not use their own teams for malicious international activity;
- States should respect the UN resolutions that are linked to human rights on the internet and to the right to privacy in the digital age

Positive duties

- States should cooperate to increase stability and security in the use of ICTs and to prevent harmful practices;
- States should consider all relevant information in case of ICT incidents;
- States should consider how best to cooperate to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs;
- States should take appropriate measures to protect their critical infrastructure;
- States should respond to appropriate requests for assistance by other states whose critical infrastructure is subject to malicious ICT acts;
- States should encourage responsible reporting of ICT vulnerabilities and should share remedies to these

Confidence building measures

Confidence building measures (CBM)

Cooperative measures

- ✓ **Establishing Points of Contacts (policy, diplomatic and technical levels)**
- ✓ **Dialogue and consultation (bilateral, regional, international, and multistakeholder – esp. among CERTs)**

Transparency measures

- ✓ **Share views on emerging threats, through publicly available decisions**
- ✓ **Share information, good practices and national policies and strategies**
- ✓ **Protect critical infrastructure, including through multistakeholder cooperation and information sharing**

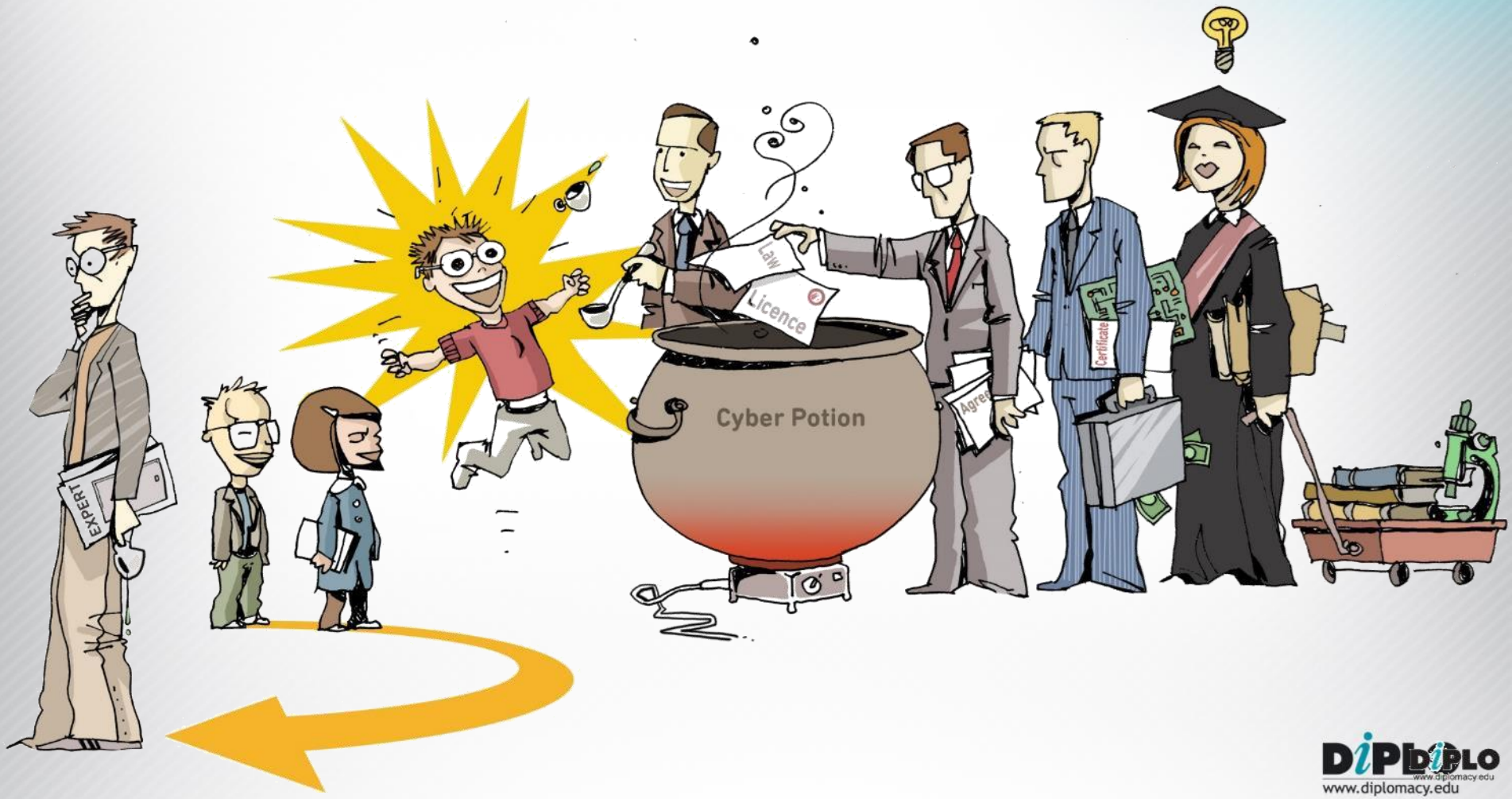
Regional CBMs

Source: OSCE

Capacity building

DiPLO
www.diplomacy.edu

Capacity building and competences



Capacity building principles (OEWG 2021)

- ✓ Sustainable process involving diversity of actors
- ✓ Clear purpose and result oriented
- ✓ Support open, secure, stable, accessible and peaceful ICT environment
- ✓ Evidence-based, politically neutral, transparent, accountable, and without conditions
- ✓ Respecting the principle of State sovereignty
- ✓ Allowing access to relevant technologies
- ✓ Participation on voluntary basis
- ✓ Based on mutual trust, demand-driven, correspond to nationally identified needs and priorities, and be undertaken in full recognition of national ownership
- ✓ Tailored to specific needs and contexts
- ✓ Active partners with different responsibilities
- ✓ Protecting confidentiality of national policies and sensitive information
- ✓ Respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory

Part III
Processes

Multilateral and multistakeholder fora

WORLD ECONOMIC FORUM

PARIS CALL
For trust and security in cyberspace

TECH ACCORD

GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE

Geneva Dialogue

FIRST
Improving Security Together

GFCE

Charter of Trust
charter-of-trust.com

OSCE

OECD

IGF Internet Governance Forum

COMITE INTERNATIONAL GENEVE

FREEDOM ONLINE COALITION

DiPLO
www.diplomacy.edu

Example: Global Commission

1. Norm to Protect the Public Core of the Internet
2. Norm to Protect the Electoral Infrastructure
3. Norm to Avoid Tampering
4. Norm Against Commandeering of ICT Devices into Botnets
5. Norm for States to Create a Vulnerabilities Equities Process
6. Norm to Reduce and Mitigate Significant Vulnerabilities
7. Norm on Basic Cyber Hygiene as Foundational Defense
8. Norm Against Offensive Cyber Operations by Non-State Actors

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

1. Ownership for cyber and IT security
2. Responsibility throughout the digital supply chain
3. Security by default
4. User-centricity
5. Innovation and co-creation
6. Education
7. Certification for critical infrastructure and solutions
8. Transparency and response
9. Regulatory framework
10. Joint initiatives

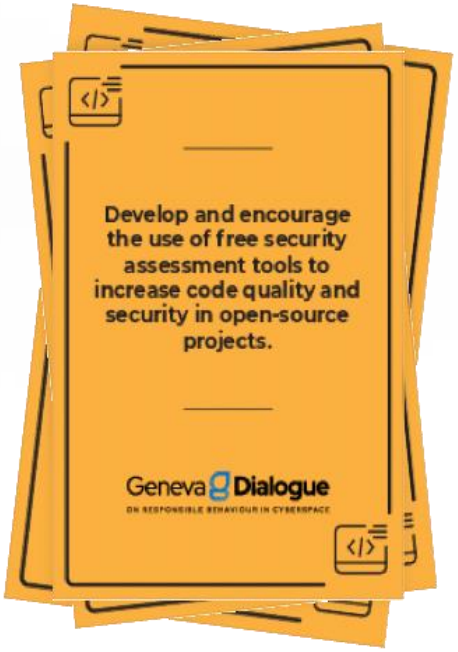
Charter of Trust
We are signing for Cybersecurity

DiPLO
www.diplomacy.edu

Example: Paris Call

- **Principle** 1. Protect individuals and infrastructure.
- **Principle** 2. Protect the Internet.
- **Principle** 3. Defend electoral processes.
- **Principle** 4. Defend intellectual property.
- **Principle** 5. Non-proliferation.
- **Principle** 6. Lifecycle security
- **Principle** 7. Cyber hygiene.
- **Principle** 8. No private hack back.
- **Principle 9.** Promote international norms

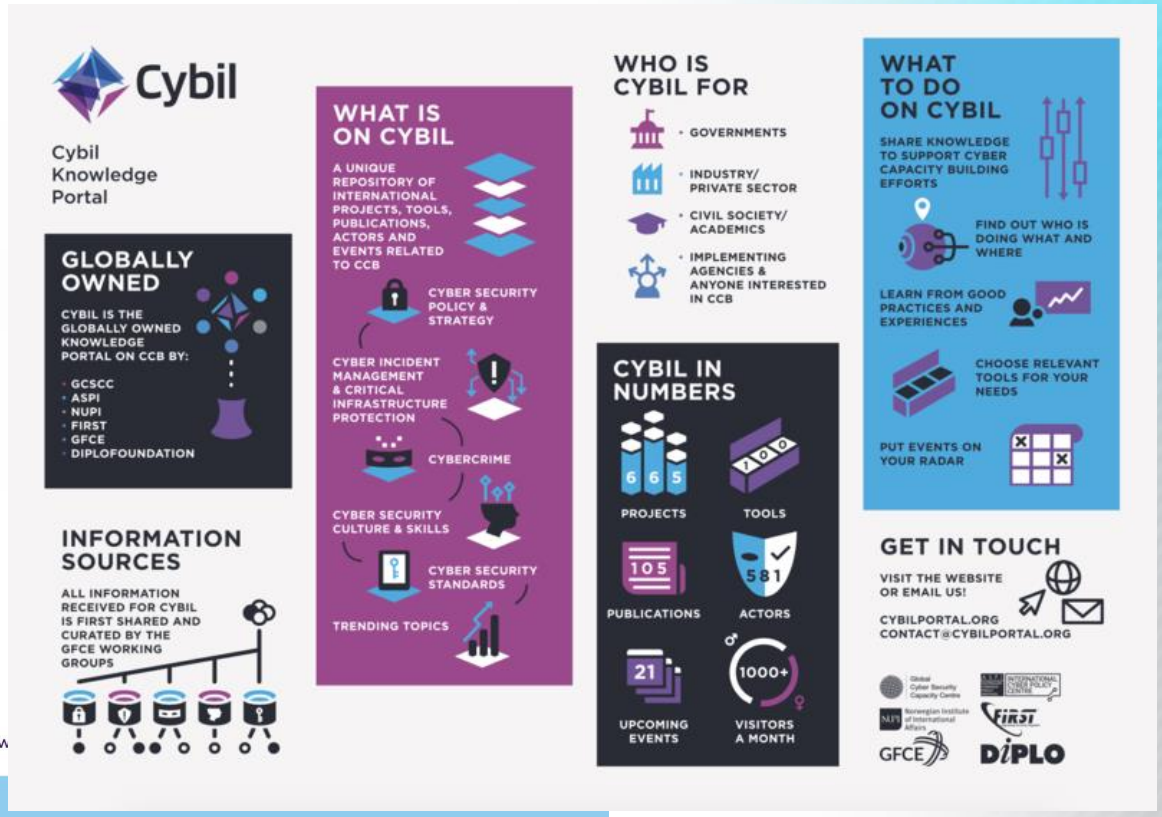
Example: Geneva Dialogue

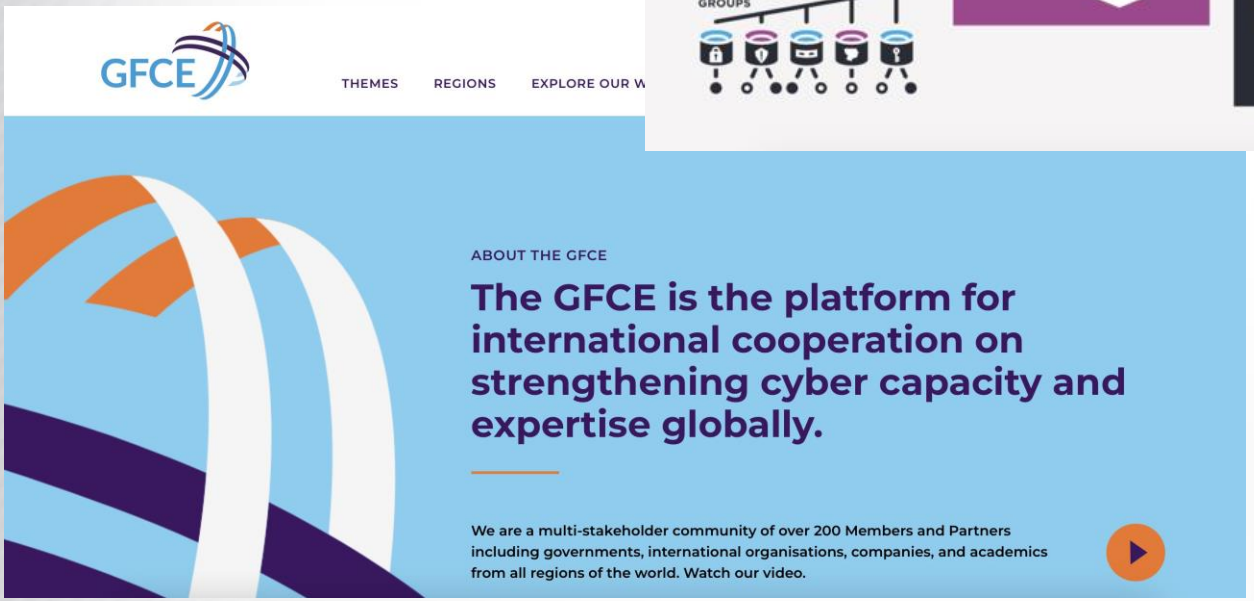


Geneva Dialogue
ON RESPONSIBLE BEHAVIOUR IN CYBERSPACE

DiPLO
www.diplomacy.edu

Example: GFCE





DiPLO
www.diplomacy.edu

Visit:
www.diplomacy.edu/cybersecurity
www.diplomacy.edu/courses
dig.watch

Contact:
diplo@diplomacy.edu
vladar@diplomacy.edu

Twitter:
@DiplomacyEdu
@vradunovic

DiPLO
www.diplomacy.edu