



# Cyber Diplomacy Workshop Programme

15<sup>th</sup>-16<sup>th</sup> 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





## Ooops, your files have been encrypted!

English

### What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

### Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

### How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

CMT from Mondays to Fridays

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)

Send \$300 worth of bitcoin to this address:



12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Woldwide, 15 May 2017, morning

Check Payment

Decrypt



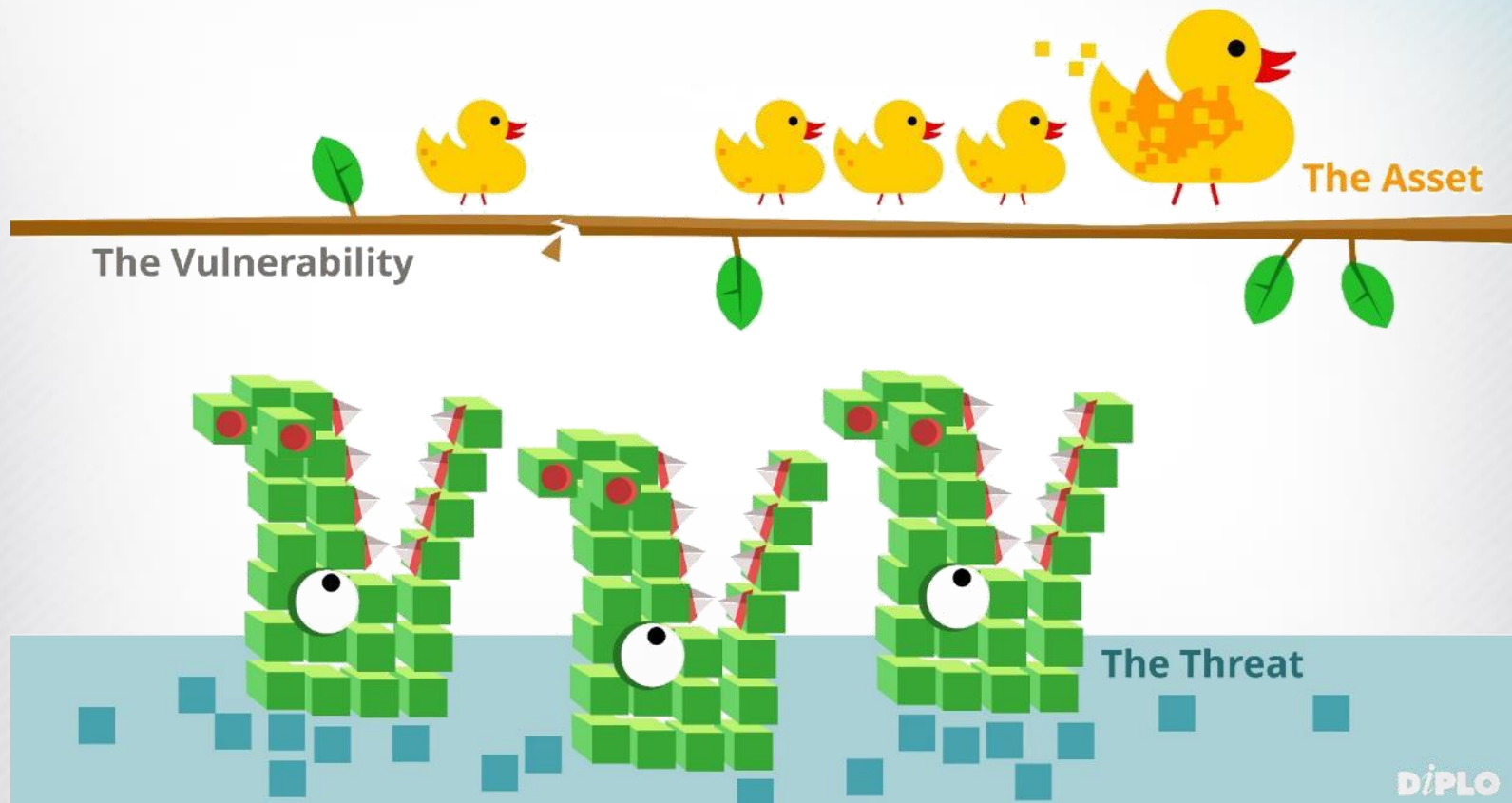


Copenhagen, 27 June 2017, 8:15

# Geopolitical Risks



# Risks

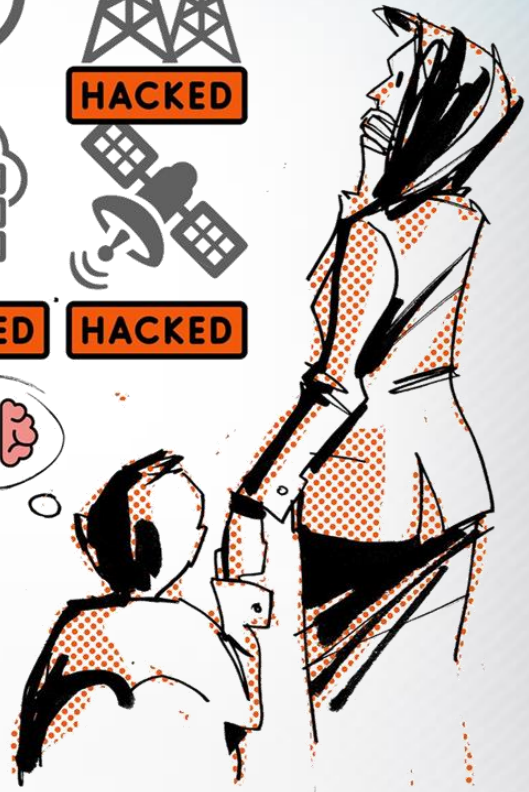


$$\text{Risk} = \text{Assets} \times \text{Threats} \times \text{Vulnerabilities}$$

# Assets



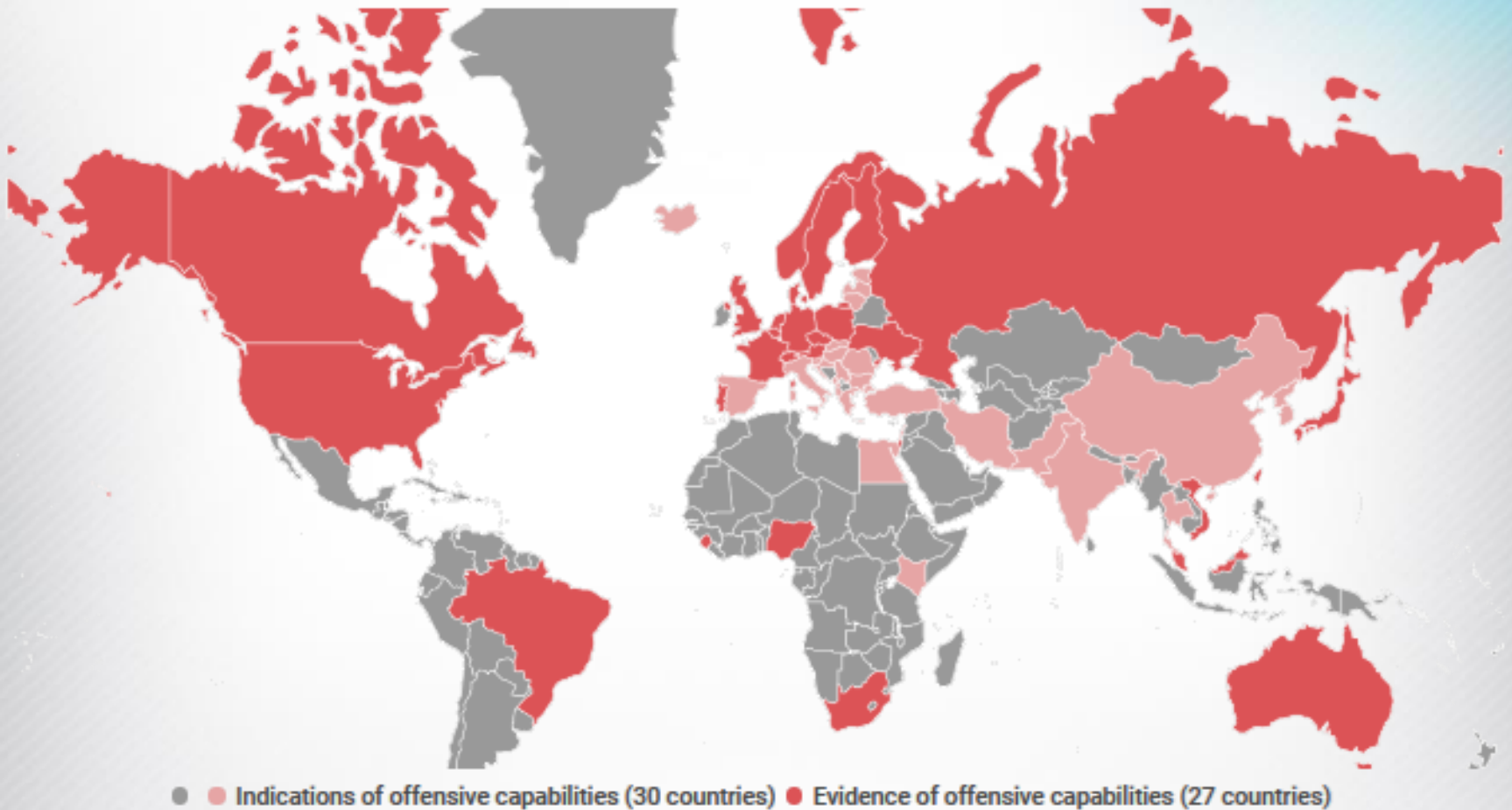
Oh!



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

# Threats

## Offensive cyber capabilities



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



# Cybersecurity Issues

# Cyber-warfare



# Disinformation



# Cybercrime

# DARK WEB





# Cyber espionage and surveillance



# AI and cybersecurity: Autonomous Lethal Weapons

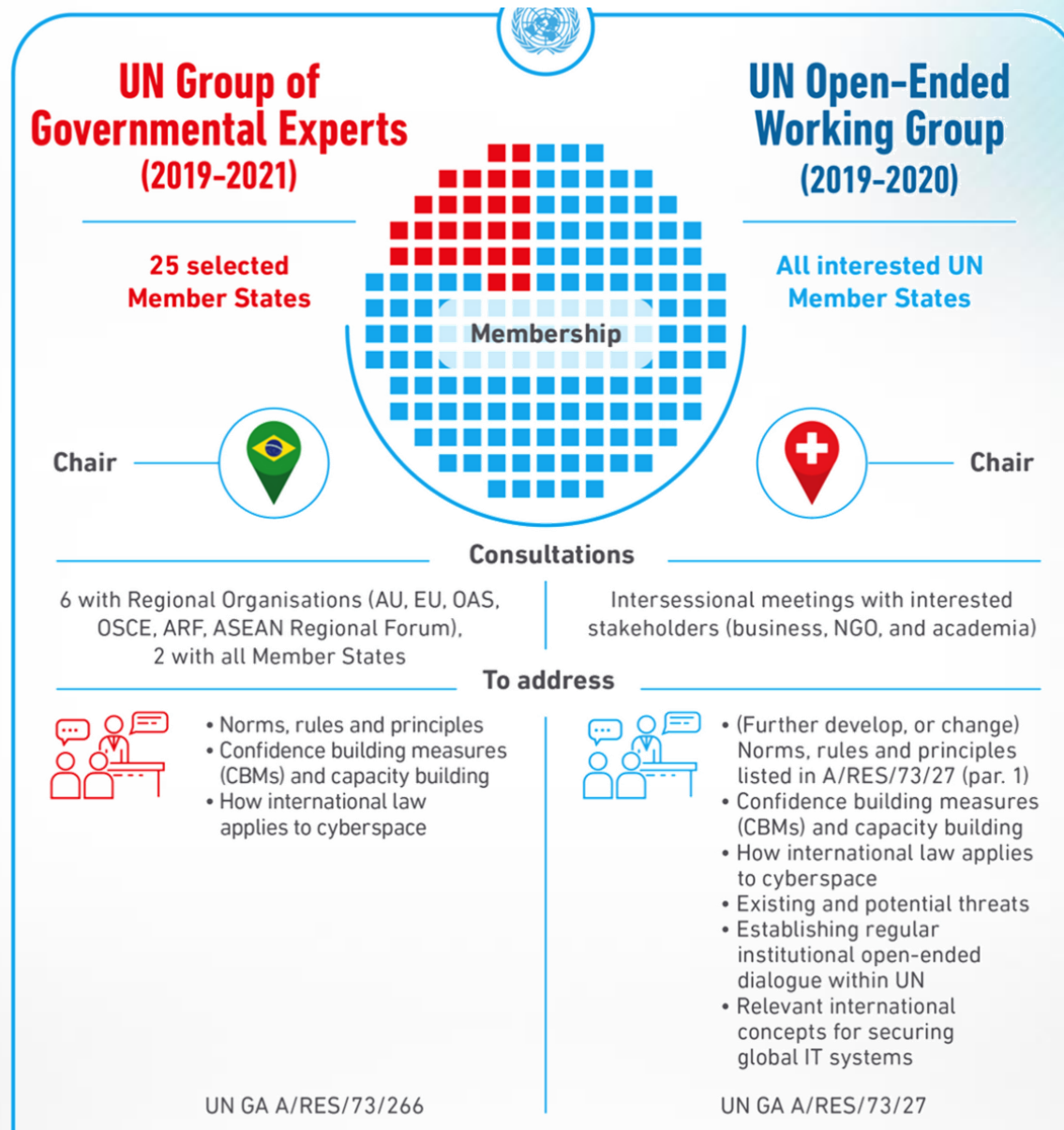


Watch: <https://www.youtube.com/watch?v=LLQUDoT95Yg>

# Part II

## Framework

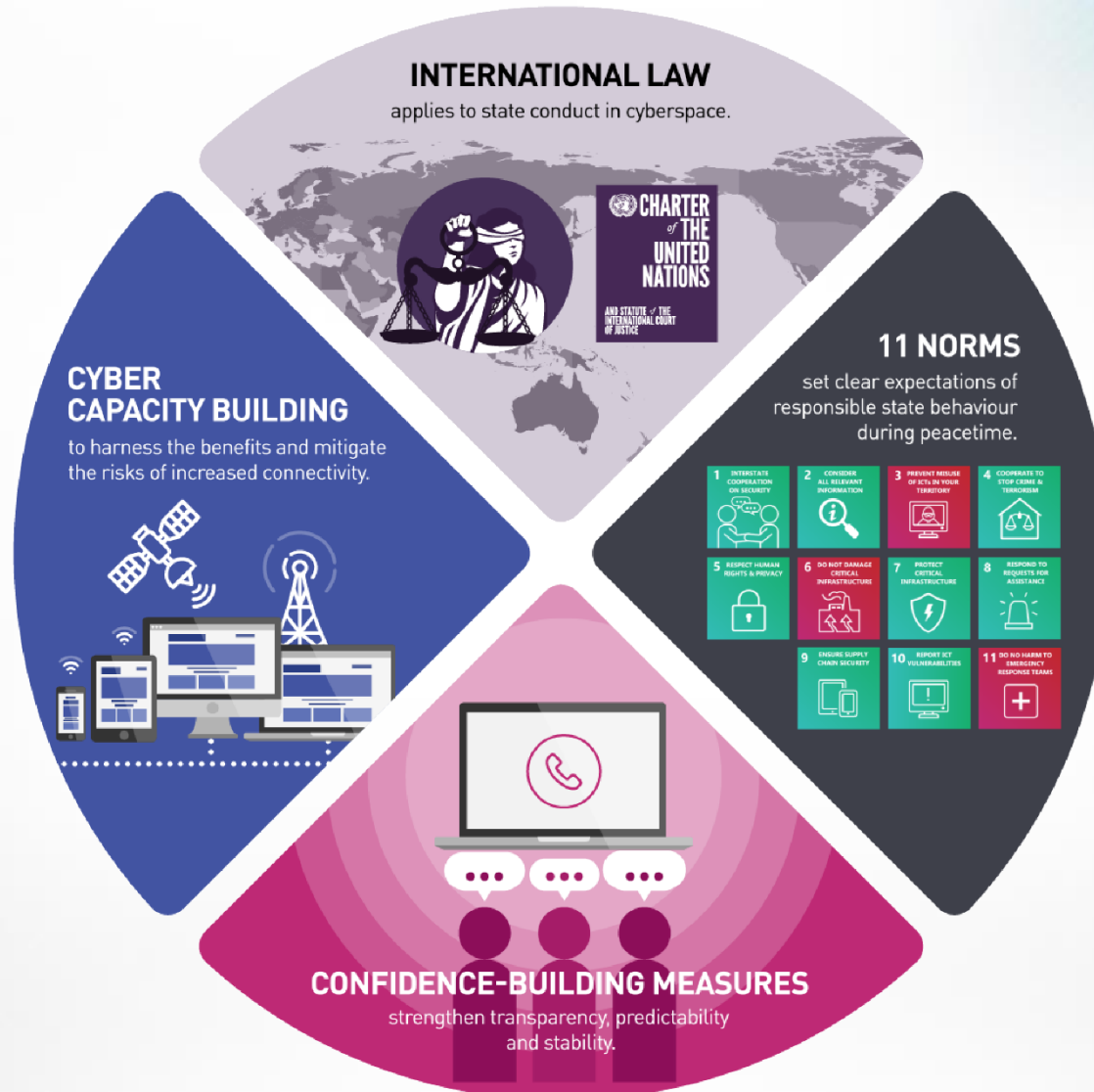
# History



Source: <https://dig.watch/ungge>



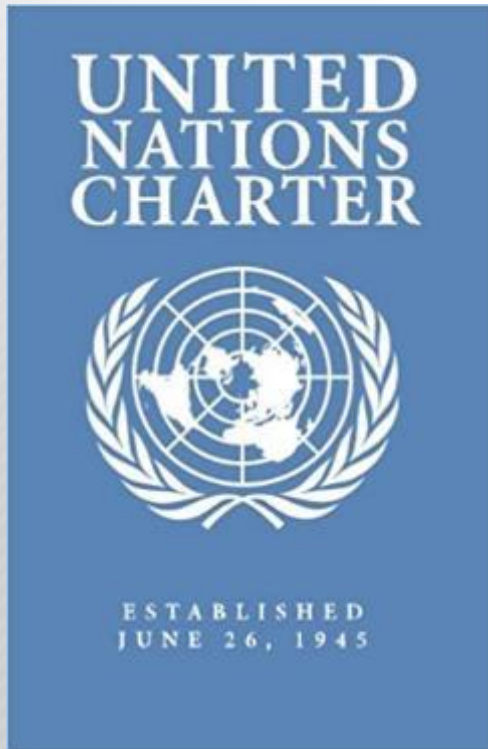
# UN framework of responsible state behaviour in cyberspace



Source: ASPI

# 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

## UN NORMS OF RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE



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**

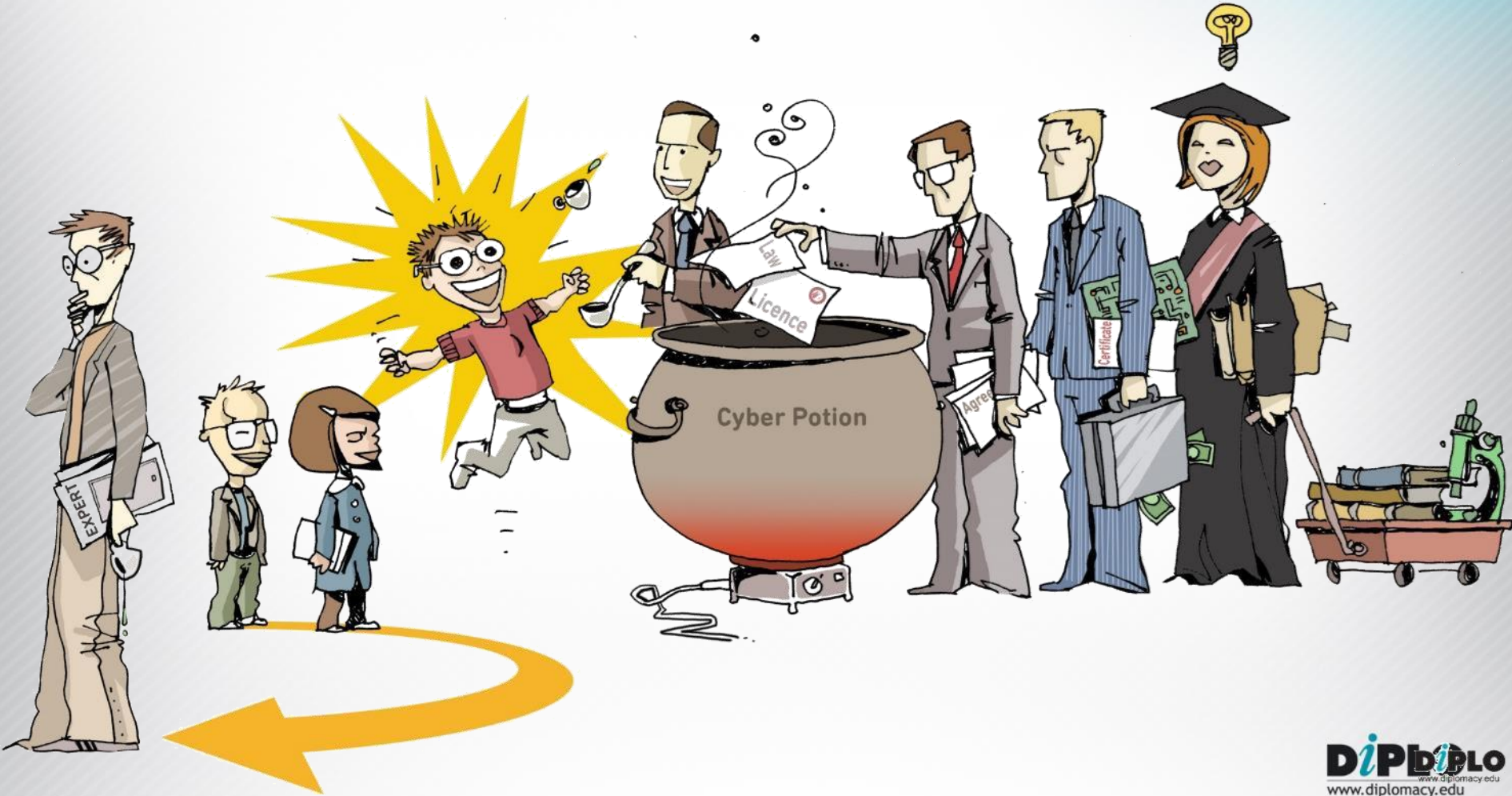
# Regional CBMs

## OSCE CYBER/ICT SECURITY CBMs

<b>1</b> Threat information sharing 	<b>2</b> Cross-border co-operation 	<b>3</b> Hold consultations 	<b>4</b> Open, interoperable, secure, and reliable Internet 	<b>5</b> Capacity building platform 	<b>6</b> Legislation to facilitate co-operation 	<b>7</b> National strategies, policies and programs 	<b>8</b> Points of Contact 
<b>9</b> ICT terminologies 	<b>10</b> OSCE platforms for exchange 	<b>11</b> Regular IWG meetings 	<b>12</b> Act jointly to reduce tensions 	<b>13</b> Effective communication channels 	<b>14</b> Public-Private Partnerships (PPPs) 	<b>15</b> Critical infrastructure protection 	<b>16</b> Sharing vulnerability information 

# Capacity building

# 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



# 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**

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



**GLOBAL COMMISSION**  
ON THE STABILITY OF CYBERSPACE



We are signing  
for Cybersecurity



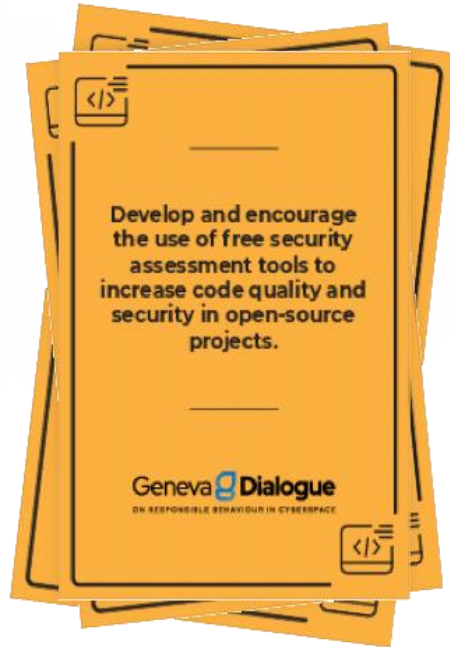
# Example: Paris Call

PARIS CALL

For trust and security in cyberspace

- **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



# Example: GFCE

**Cybil Knowledge Portal**

**GLOBALY OWNED**  
 CYBIL IS THE GLOBALLY OWNED KNOWLEDGE PORTAL ON CCB BY:  
 - GCSCC  
 - ASPI  
 - NUPI  
 - FIRST  
 - GFCE  
 - DIPLOFOUNDATION

**WHAT IS ON CYBIL**  
 A UNIQUE REPOSITORY OF INTERNATIONAL PROJECTS, TOOLS, PUBLICATIONS, ACTORS AND EVENTS RELATED TO CCB

- CYBER SECURITY POLICY & STRATEGY
- CYBER INCIDENT MANAGEMENT & CRITICAL INFRASTRUCTURE PROTECTION
- CYBERCRIME
- CYBER SECURITY CULTURE & SKILLS
- CYBER SECURITY STANDARDS
- TRENDING TOPICS

**WHO IS CYBIL FOR**

- GOVERNMENTS
- INDUSTRY/PRIVATE SECTOR
- CIVIL SOCIETY/ACADEMICS
- IMPLEMENTING AGENCIES & ANYONE INTERESTED IN CCB

**WHAT TO DO ON CYBIL**  
 SHARE KNOWLEDGE TO SUPPORT CYBER CAPACITY BUILDING EFFORTS  
 FIND OUT WHO IS DOING WHAT AND WHERE  
 LEARN FROM GOOD PRACTICES AND EXPERIENCES  
 CHOOSE RELEVANT TOOLS FOR YOUR NEEDS  
 PUT EVENTS ON YOUR RADAR

**INFORMATION SOURCES**  
 ALL INFORMATION RECEIVED FOR CYBIL IS FIRST SHARED AND CURATED BY THE GFCE WORKING GROUPS

**CYBIL IN NUMBERS**

- PROJECTS: 665
- TOOLS: 700
- PUBLICATIONS: 105
- ACTORS: 581
- UPCOMING EVENTS: 21
- VISITORS A MONTH: 1000+

**GET IN TOUCH**  
 VISIT THE WEBSITE OR EMAIL US!  
 CYBILPORTAL.ORG  
 CONTACT@CYBILPORTAL.ORG

Global Cyber Security Capacity Centre  
 Norwegian Institute of International Affairs  
 GFCE  
 DIPLO

THEMES    REGIONS    EXPLORE OUR W

ABOUT THE GFCE

**The GFCE is the platform for international cooperation on strengthening cyber capacity and expertise globally.**

We are a multi-stakeholder community of over 200 Members and Partners including governments, international organisations, companies, and academics from all regions of the world. Watch our video.

*Visit:*

[www.diplomacy.edu/cybersecurity](http://www.diplomacy.edu/cybersecurity)

[www.diplomacy.edu/courses](http://www.diplomacy.edu/courses)

[dig.watch](http://dig.watch)

*Contact:*

[diplo@diplomacy.edu](mailto:diplo@diplomacy.edu)

[vladar@diplomacy.edu](mailto:vladar@diplomacy.edu)

*Twitter:*

[@DiplomacyEdu](https://twitter.com/DiplomacyEdu)

[@vradunovic](https://twitter.com/vradunovic)

***di*PLO**  

---

[www.diplomacy.edu](http://www.diplomacy.edu)