Geneva Dialogue

ON RESPONSIBLE BEHAVIOUR IN CYBERSPACE

The Role of Non-State Stakeholders in the Implementation of Norms

Non-State Actors, the UN Framework
and Critical Infrastructure

Serge Droz
serge.droz@first.org

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

DiPLO

REPUBLIC
AND STATE
OF GENEVA

EPFL CENTER FOR
DIGITAL TRUST

UBS

swisscom

Geneva Dialogue

ON RESPONSIBLE BEHAVIOUR IN CYBERSPACE

The Geneva Dialogue endeavours to:

Facilitate an inclusive global dialogue on the roles and responsibilities in cyberspace

Geneva Dialogue

ON RESPONSIBLE BEHAVIOUR IN CYBERSPACE

PRIVATE SECTOR AND INDUSTRY

ACADEMIA

4 STAKEHOLDER GROUPS

CIVIL SOCIETY

TECHNICAL COMMUNITY
(including open-source community, cybersecurity researchers and incident response experts)

FACILITATING AN INCLUSIVE GLOBAL DIALOGUE TO MAP ROLES AND RESPONSIBILITY OF NON-STATE STAKEHOLDERS IN CYBERSPACE AND IMPLEMENT AGREED CYBER NORMS

69 CONTRIBUTORS IN 2023-2024

to the Geneva Dialogue representing both organisations and individual experts from

21 COUNTRIES

and

ALL REGIONS

2 CHAPTERS OF

the Geneva Manual on Responsible Behaviour in Cyberspace focused on

5 AGREED UN GGE CYBER NORMS:

- supply chain security (Norm I)
- responsible reporting of ICT vulnerabilities (Norm J)
- protection of critical infrastructure (Norms F, G, and H)

Geneva Dialogue

ON RESPONSIBLE BEHAVIOUR IN CYBERSPACE

2018

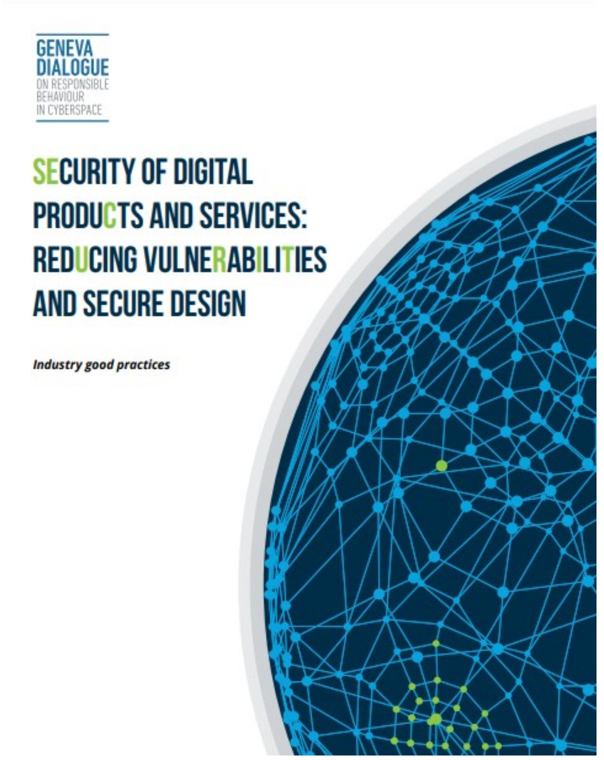
Inauguration

First discussions to explore responsibilities of States and other actors in cyberspace.

2020

Output report

Focus on **industry responsibilities** to reduce vulnerabilities and build secure products.


GENEVA DIALOGUE
ON RESPONSIBLE BEHAVIOUR IN CYBERSPACE

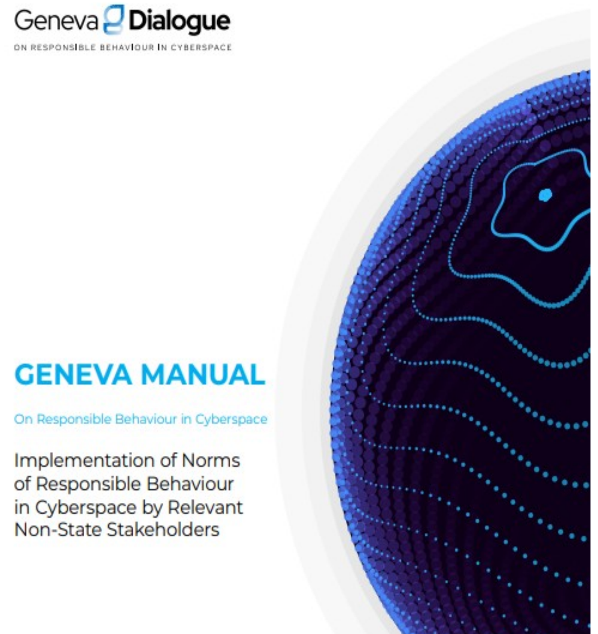
SECURITY OF DIGITAL PRODUCTS AND SERVICES: REDUCING VULNERABILITIES AND SECURE DESIGN

Industry good practices

2023

Geneva Manual: Chapter I

Focus on the two norms on **ICT supply chain security and vulnerabilities.**


Geneva Dialogue
ON RESPONSIBLE BEHAVIOUR IN CYBERSPACE

GENEVA MANUAL

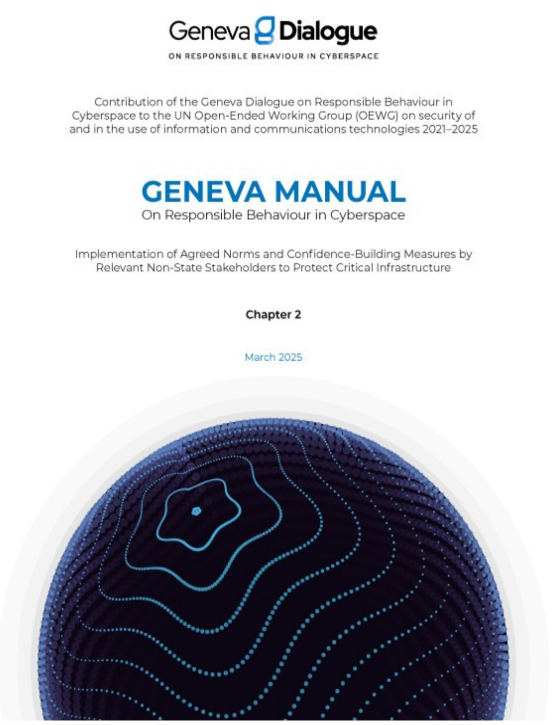
On Responsible Behaviour in Cyberspace

Implementation of Norms
of Responsible Behaviour
in Cyberspace by Relevant
Non-State Stakeholders

2025

Geneva Manual: Chapter II

Implementation of the norms and CBMs to **protect critical infrastructure**.


Geneva Dialogue
ON RESPONSIBLE BEHAVIOUR IN CYBERSPACE

Contribution of the Geneva Dialogue on Responsible Behaviour in Cyberspace to the UN Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies 2021–2025

GENEVA MANUAL

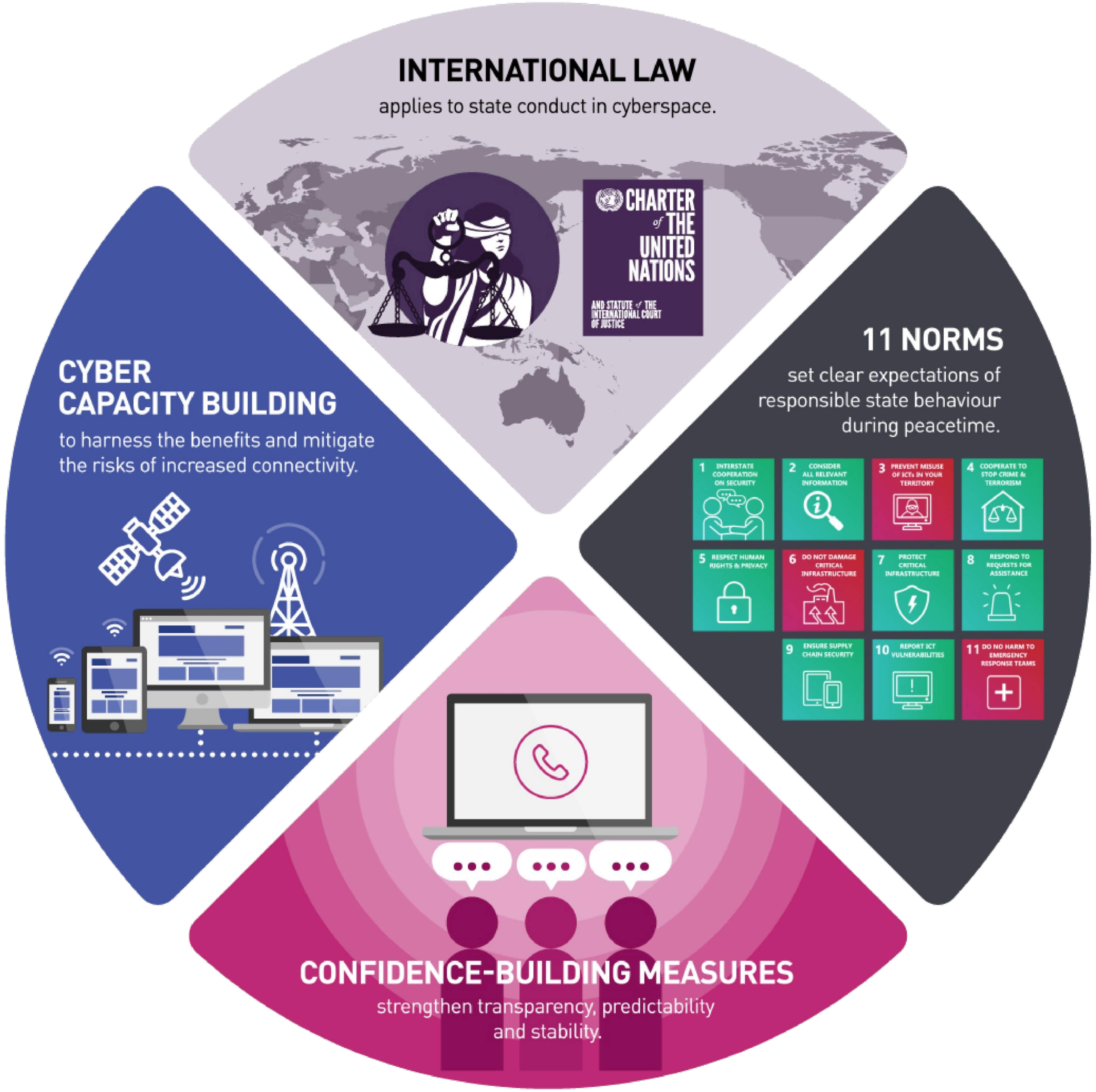
On Responsible Behaviour in Cyberspace

Implementation of Agreed Norms and Confidence-Building Measures by Relevant Non-State Stakeholders to Protect Critical Infrastructure

Chapter 2

March 2025

Who is responsible for protecting critical infrastructure?



INTERNATIONAL LAW
applies to state conduct in cyberspace.

CHARTER of THE UNITED NATIONS
AND STATUTE of THE INTERNATIONAL COURT OF JUSTICE

11 NORMS
set clear expectations of responsible state behaviour during peacetime.

1 INTERSTATE COOPERATION ON SECURITY
2 CONSIDER ALL RELEVANT INFORMATION
3 PREVENT MISUSE OF ICTs IN YOUR TERRITORY
4 COOPERATE TO STOP CRIME & TERRORISM
5 RESPECT HUMAN RIGHTS & PRIVACY
6 DO NOT DAMAGE CRITICAL INFRASTRUCTURE
7 PROTECT CRITICAL INFRASTRUCTURE
8 RESPOND TO REQUESTS FOR ASSISTANCE
9 ENSURE SUPPLY CHAIN SECURITY
10 REPORT ICT VULNERABILITIES
11 DO NO HARM TO EMERGENCY RESPONSE TEAMS

CYBER CAPACITY BUILDING
to harness the benefits and mitigate the risks of increased connectivity.

CONFIDENCE-BUILDING MEASURES
strengthen transparency, predictability and stability.

UN Framework for Responsible State Behaviour in Cyberspace

Geneva Dialogue

ON RESPONSIBLE BEHAVIOUR IN CYBERSPACE

- A INTERSTATE CO-OPERATION ON SECURITY
- B CONSIDER ALL RELEVANT INFORMATION
- C PREVENT MISUSE OF ICTS IN YOUR TERRITORY
- D COOPERATE TO STOP CRIME AND TERRORISM
- E RESPECT HUMAN RIGHTS AND PRIVACY
- F DO NOT DAMAGE CRITICAL INFRASTRUCTURE
- G PROTECT CRITICAL INFRASTRUCTURE
- H RESPOND TO REQUESTS FOR ASSISTANCE
- I ENSURE SUPPLY CHAIN SECURITY
- J REPORT ICT VULNERABILITIES
- K DO NO HARM TO RESPONSE TEAMS

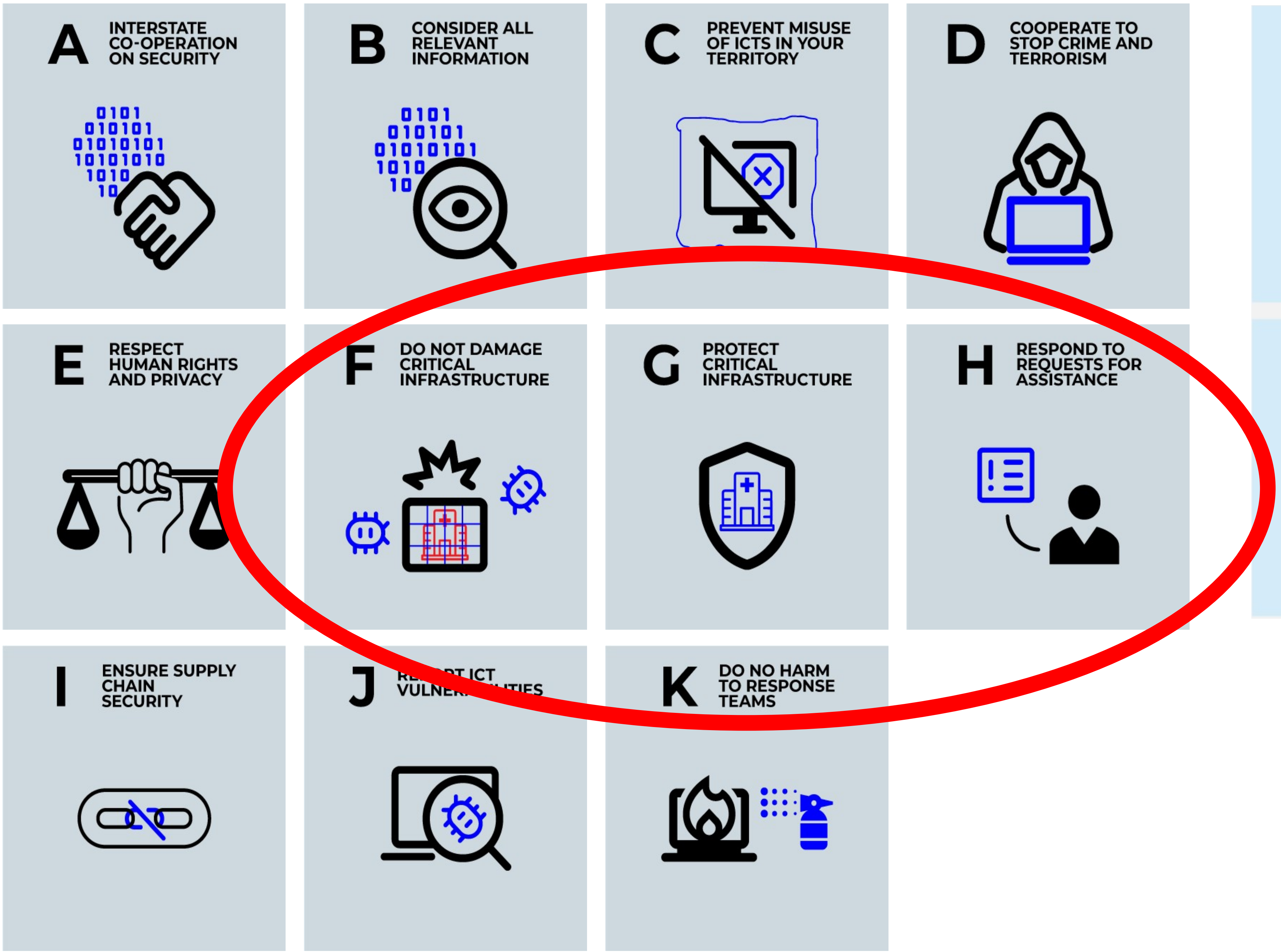
Voluntary norms

- NATIONAL POINTS OF CONTACT
- EXCHANGING NATIONAL VIEWS
- SHARING INFORMATION ON A VOLUNTARY BASIS
- COOPERATIVE EXERCISE OF CBMs
- CAPACITY BUILDING IN ICT SECURITY
- REGULAR SEMINARS, WORKSHOPS AND TRAINING PROGRAMMES ON ICT SECURITY
- EXCHANGING INFORMATION ON THE PROTECTION OF CI AND CII
- PUBLIC-PRIVATE PARTNERSHIPS ON ICT SECURITY

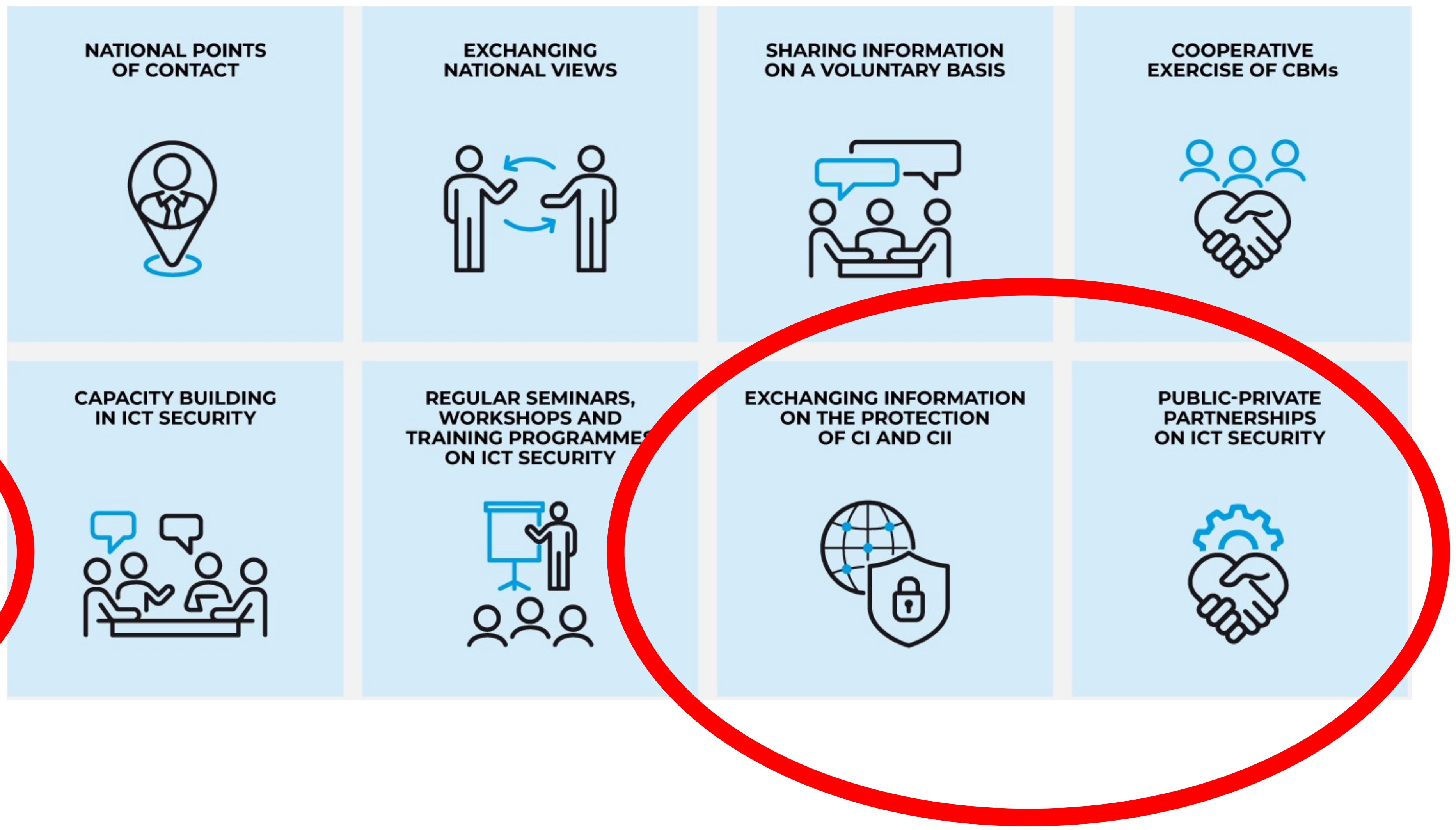
Confidence-building measures

Geneva Dialogue

ON RESPONSIBLE BEHAVIOUR IN CYBERSPACE



A INTERSTATE CO-OPERATION ON SECURITY
B CONSIDER ALL RELEVANT INFORMATION
C PREVENT MISUSE OF ICTS IN YOUR TERRITORY
D COOPERATE TO STOP CRIME AND TERRORISM
E RESPECT HUMAN RIGHTS AND PRIVACY
F DO NOT DAMAGE CRITICAL INFRASTRUCTURE
G PROTECT CRITICAL INFRASTRUCTURE
H RESPOND TO REQUESTS FOR ASSISTANCE
I ENSURE SUPPLY CHAIN SECURITY
J REPORT ICT VULNERABILITIES
K DO NO HARM TO RESPONSE TEAMS



NATIONAL POINTS OF CONTACT
EXCHANGING NATIONAL VIEWS
SHARING INFORMATION ON A VOLUNTARY BASIS
COOPERATIVE EXERCISE OF CBMs
CAPACITY BUILDING IN ICT SECURITY
REGULAR SEMINARS, WORKSHOPS AND TRAINING PROGRAMMES ON ICT SECURITY
EXCHANGING INFORMATION ON THE PROTECTION OF CI AND CII
PUBLIC-PRIVATE PARTNERSHIPS ON ICT SECURITY

Voluntary norms

Confidence-building measures

How do cyber norms guide actors in protecting CI?

How are non-state stakeholders expected to implement the norms?

How do non-state stakeholders understand the implementation of the cyber norms and CBMs to protect critical infrastructure?

Responsibilities

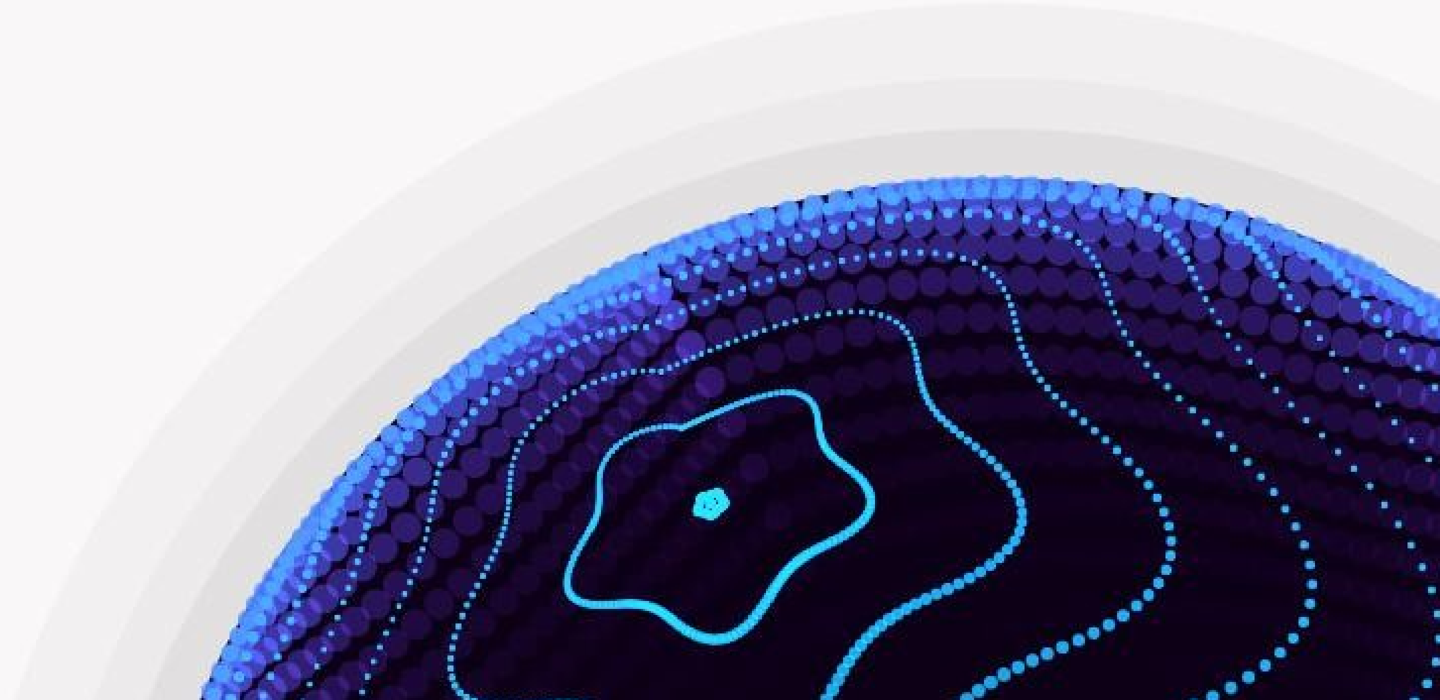
Incentives

Challenges

Good practices

- CI operators/owners
- Open-source software (OSS) community
- Product vendors and service providers
- Cybersecurity researchers, Incident response experts
- Civil society

Key messages



#1

More international action is needed to understand and protect cross-border interdependencies in certain critical infrastructure sectors that have regional and global impact.

#2

Secrecy in defining CI for national security reasons limits the awareness of stakeholders to support states' efforts in CIP.

#3

The absence of common minimum cybersecurity standards for critical infrastructure limits progress toward cyber resilience.

#4

Challenges in managing vulnerabilities in industrial control systems (ICS) leave critical infrastructure exposed to hidden cybersecurity risks.

#5

Cybersecurity experts and technical teams increasingly struggle to stay politically neutral, creating risks for protecting critical infrastructure and securing ICT across borders.

#6

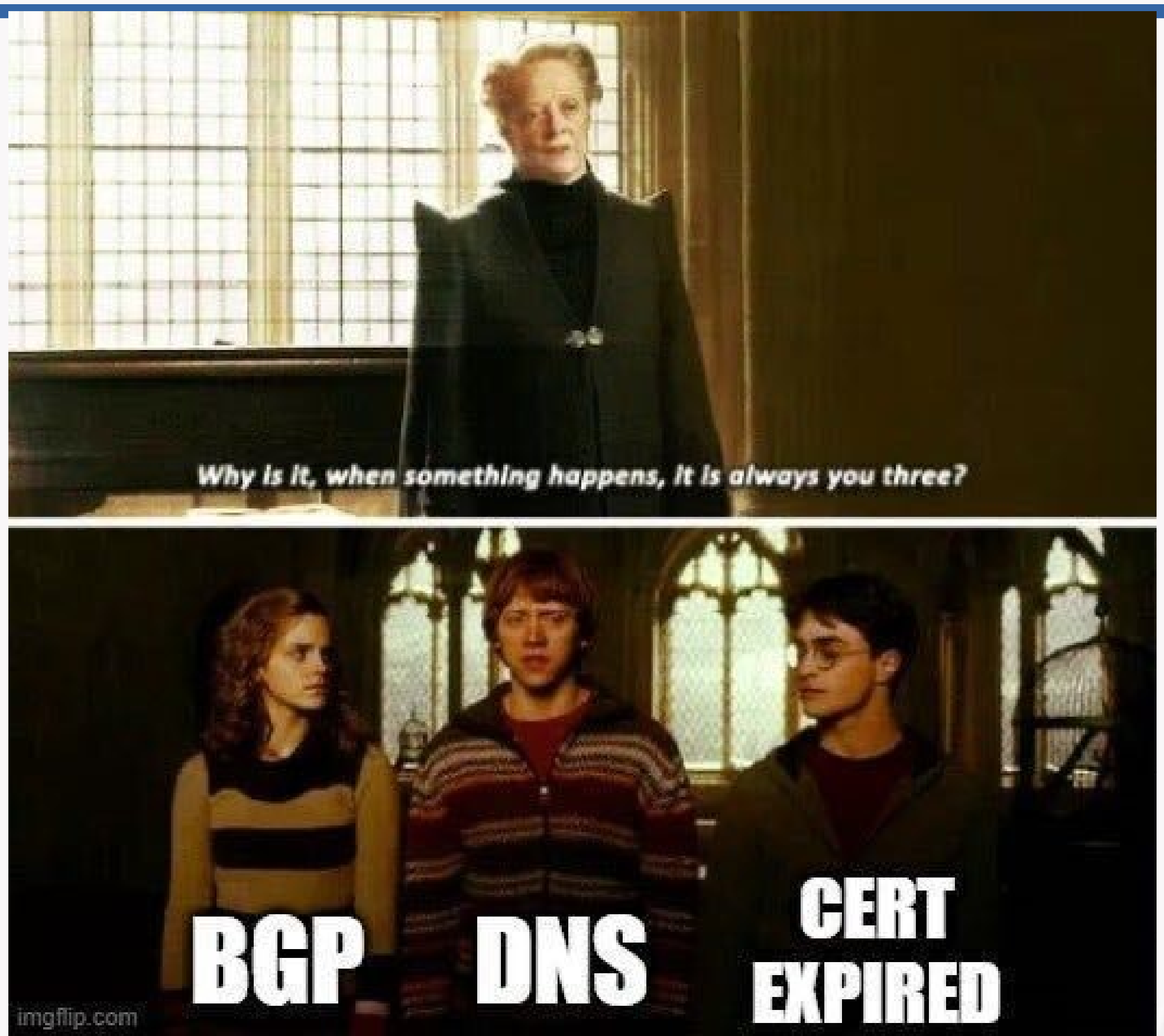
UN GGE norm F mainly focuses on intentional damage and may not fully cover other risks to critical infrastructure security.

#7

Rising inter-state conflicts highlight the need for governments to give clear legal guidance to private actors involved in protecting critical infrastructure.

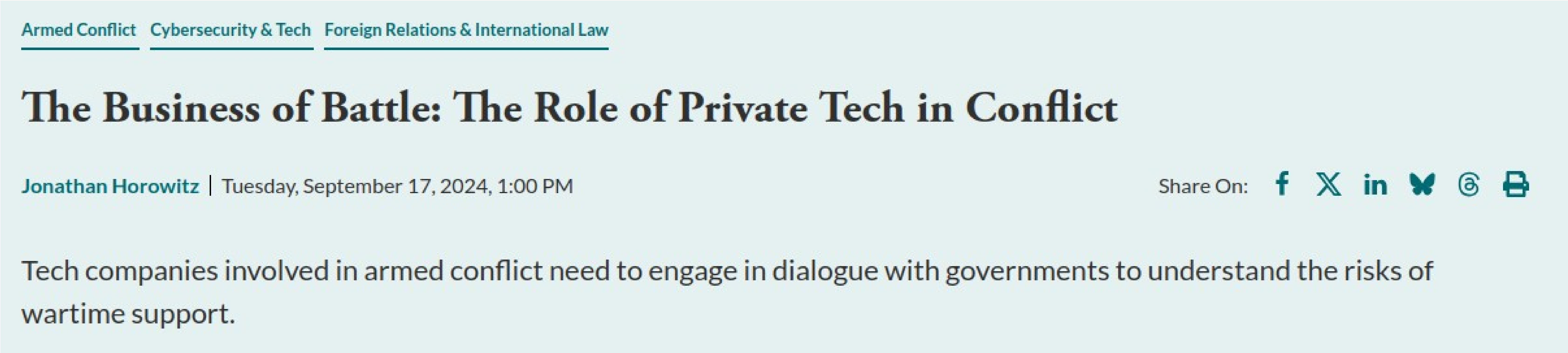
Key message #1

More international action is needed to understand and protect cross-border interdependencies in certain critical infrastructure sectors that have regional and global impact.



Key message #7

The increase in inter-state conflicts underscores the need for states to provide clear legal guidance to private entities, helping to protect them and support their efforts in CIP.



Armed Conflict Cybersecurity & Tech Foreign Relations & International Law

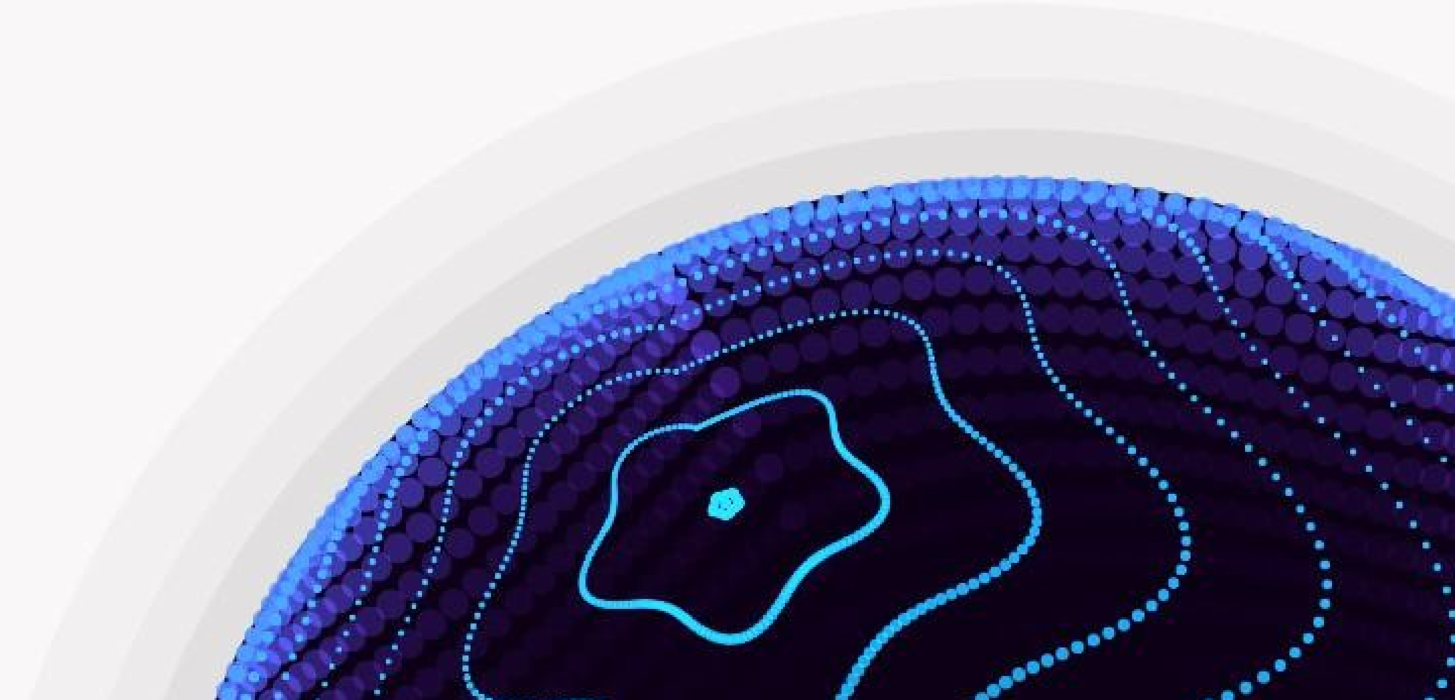
The Business of Battle: The Role of Private Tech in Conflict

Jonathan Horowitz | Tuesday, September 17, 2024, 1:00 PM

Share On:

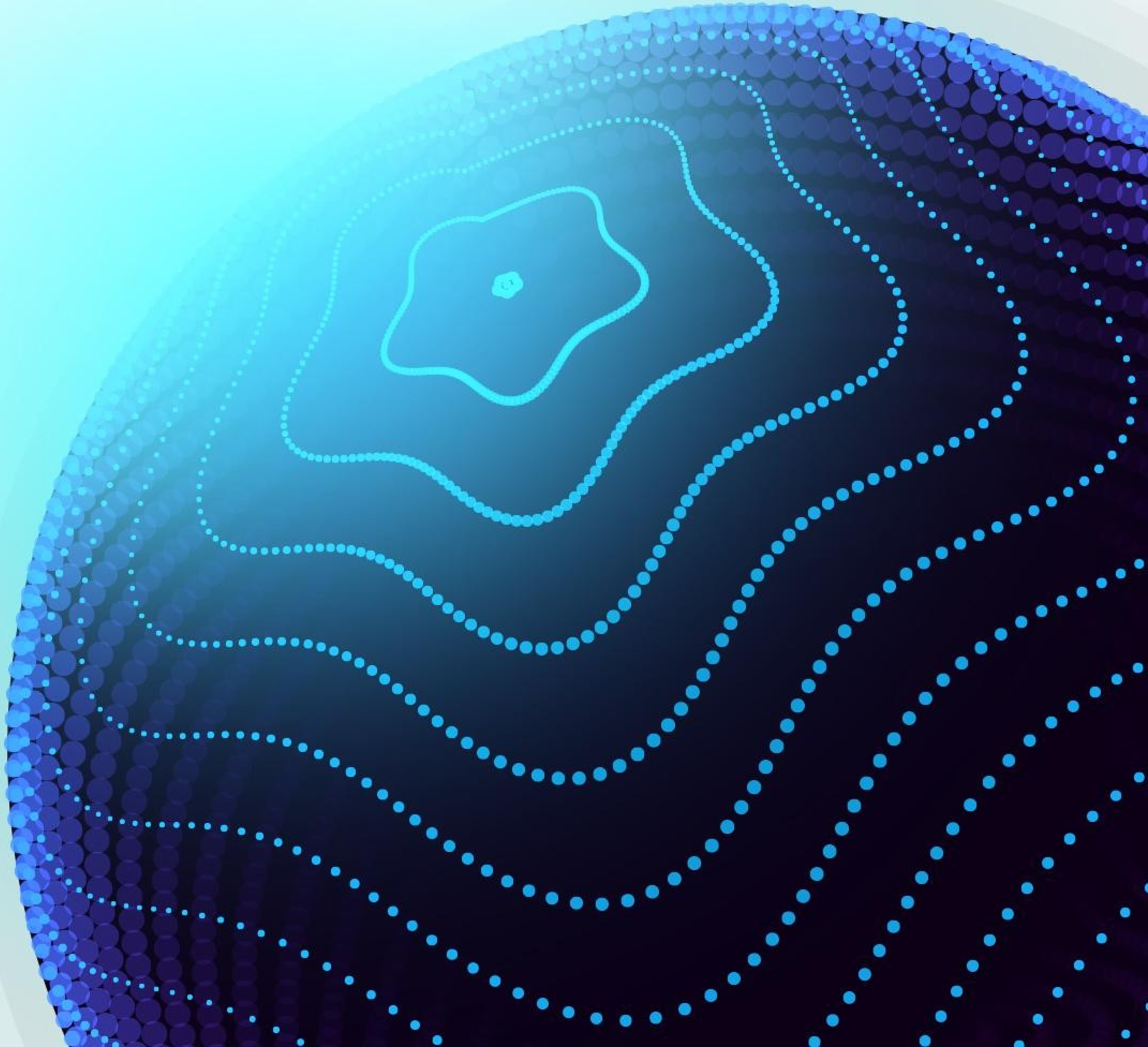
Tech companies involved in armed conflict need to engage in dialogue with governments to understand the risks of wartime support.

Contribute!
https://genevadialogue.ch/



Geneva Dialogue
ON RESPONSIBLE BEHAVIOUR IN CYBERSPACE

Thank you!



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

DiPLO

REPUBLIC
AND STATE
OF GENEVA

EPFL CENTER FOR DIGITAL TRUST

UBS

swisscom