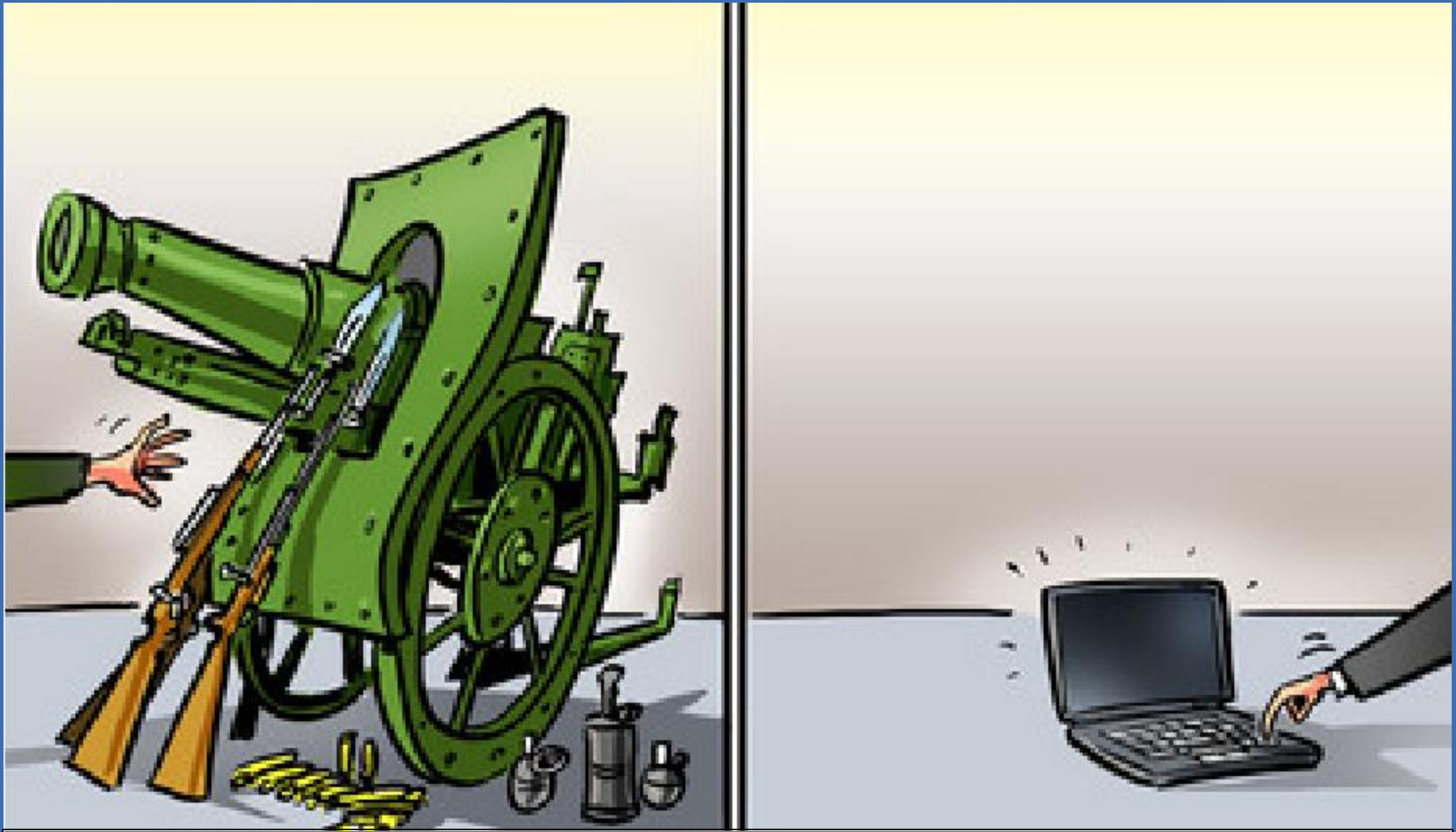
Global Conference on Space and the Information Society

Geneva, 6-7 June 2016

Karsten Geier
Head,
Cyber Policy Coordination Staff
Federal Foreign Office
Berlin, Germany

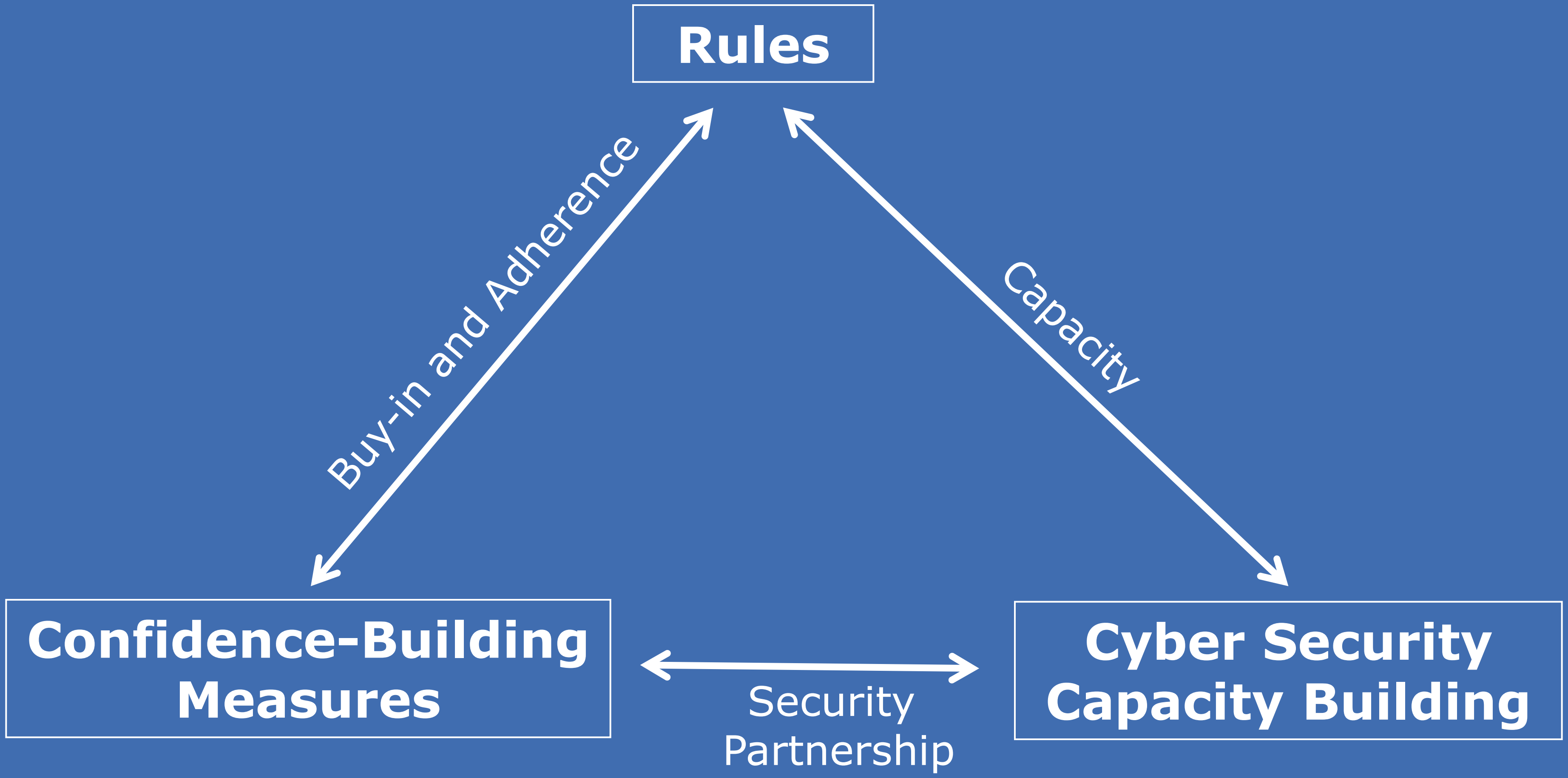
Both outer-space based and cyberspace programs can present challenges to international security.



1914

2014

A Self-Reinforcing Triangle of International Cyber Security Policy:



Rules

Buy-in and Adherence

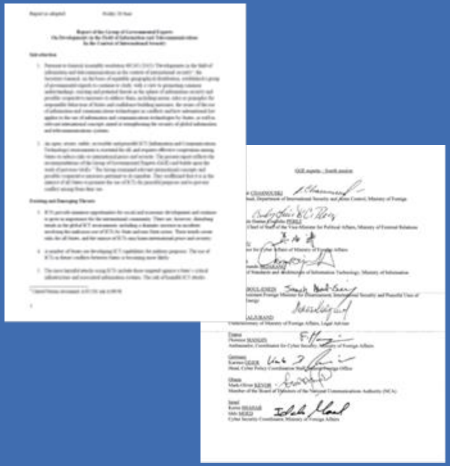
Capacity

Confidence-Building Measures

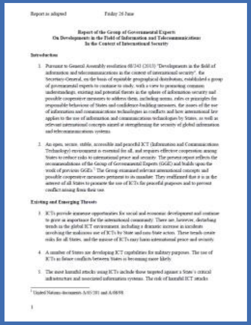
Security Partnership

Cyber Security Capacity Building

- *“International law, and in particular the UN Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.”*
- (2012/2013 Cyber GGE)



2014/2015 GGE views on how international law applies to the use of ICTs by States cover:



Report as adopted Friday 26 June

Report of the Group of Governmental Experts
On Developments in the Field of Information and Telecommunications
In the Context of International Security

Introduction

1. Pursuant to General Assembly resolution 68/243 (2013) "Developments in the field of information and telecommunications in the context of international security", the Secretary-General, on the basis of equitable geographical distribution, established a group of governmental experts to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them, including norms, rules or principles for responsible behaviour of States and confidence-building measures, the issues of the use of information and communications technologies in conflicts and how international law applies to the use of information and communications technologies by States, as well as relevant international concepts aimed at strengthening the security of global information and telecommunications systems.

2. An open, secure, stable, accessible and peaceful ICT (Information and Communications Technology) environment is essential for all, and requires effective cooperation among States to reduce risks to international peace and security. The present report reflects the recommendations of the Group of Governmental Experts (GGE) and builds upon the work of previous GGEs.[1] The Group examined relevant international concepts and possible cooperative measures pertinent to its mandate. They reaffirmed that it is in the interest of all States to promote the use of ICTs for peaceful purposes and to prevent conflict arising from their use.

Existing and Emerging Threats

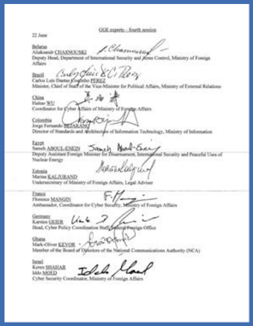
3. ICTs provide immense opportunities for social and economic development and continue to grow in importance for the international community. There are, however, disturbing trends in the global ICT environment, including a dramatic increase in incidents involving the malicious use of ICTs by State and non-State actors. These trends create risks for all States, and the misuse of ICTs may harm international peace and security.

4. A number of States are developing ICT capabilities for military purposes. The use of ICTs in future conflicts between States is becoming more likely.

5. The most harmful attacks using ICTs include those targeted against a State's critical infrastructure and associated information systems. The risk of harmful ICT attacks

[1] United Nations documents A/65/201 and A/68/98.

1



GGE experts – fourth session

22 June

Belarus
Aliaksandr CHASNOUSKI
Deputy Head, Department of International Security and Arms Control, Ministry of Foreign Affairs

Brazil
Carlos Luís Dantas Coutinho PEREZ
Minister, Chief of Staff of the Vice-Minister for Political Affairs, Ministry of External Relations

China
Haitao WU
Coordinator for Cyber Affairs of Ministry of Foreign Affairs

Colombia
Jorge Fernando BEJARANO
Director of Standards and Architecture of Information Technology, Ministry of Information

Egypt
Sameh ABOUL-ENEIN Sameh Aboul-Enein
Deputy Assistant Foreign Minister for Disarmament, International Security and Peaceful Uses of Nuclear Energy

Estonia
Marina KALJURAND
Undersecretary of Ministry of Foreign Affairs, Legal Adviser

France
Florence MANGIN
Ambassador, Coordinator for Cyber Security, Ministry of Foreign Affairs

Germany
Karsten GEIER
Head, Cyber Policy Coordination Staff, Federal Foreign Office

Ghana
Mark-Oliver KEVOR
Member of the Board of Directors of the National Communications Authority (NCA)

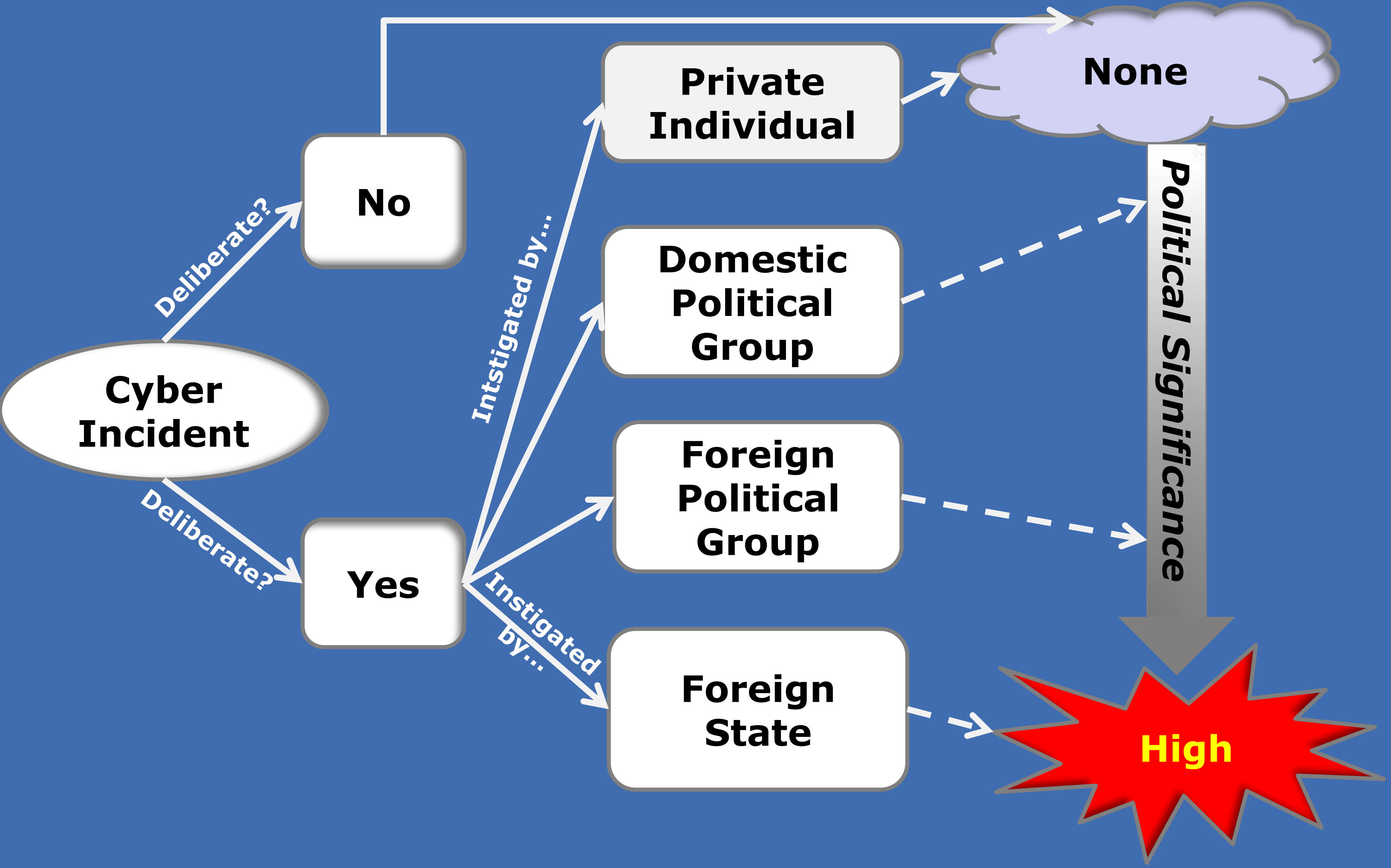
Israel
Keren SHAHAR
Iddo MOED Iddo Moed
Cyber Security Coordinator, Ministry of Foreign Affairs

- Jurisdiction over ICT infrastructure;
- State sovereignty;
- The inherent right of states to take measures consistent with international law and as recognized in the UN Charter;
- Where applicable, the principles of humanity, necessity, proportionality and distinction;
- The use of proxies; and
- International obligations regarding internationally wrongful acts.

GGE recommendations for voluntary, non-binding norms include:

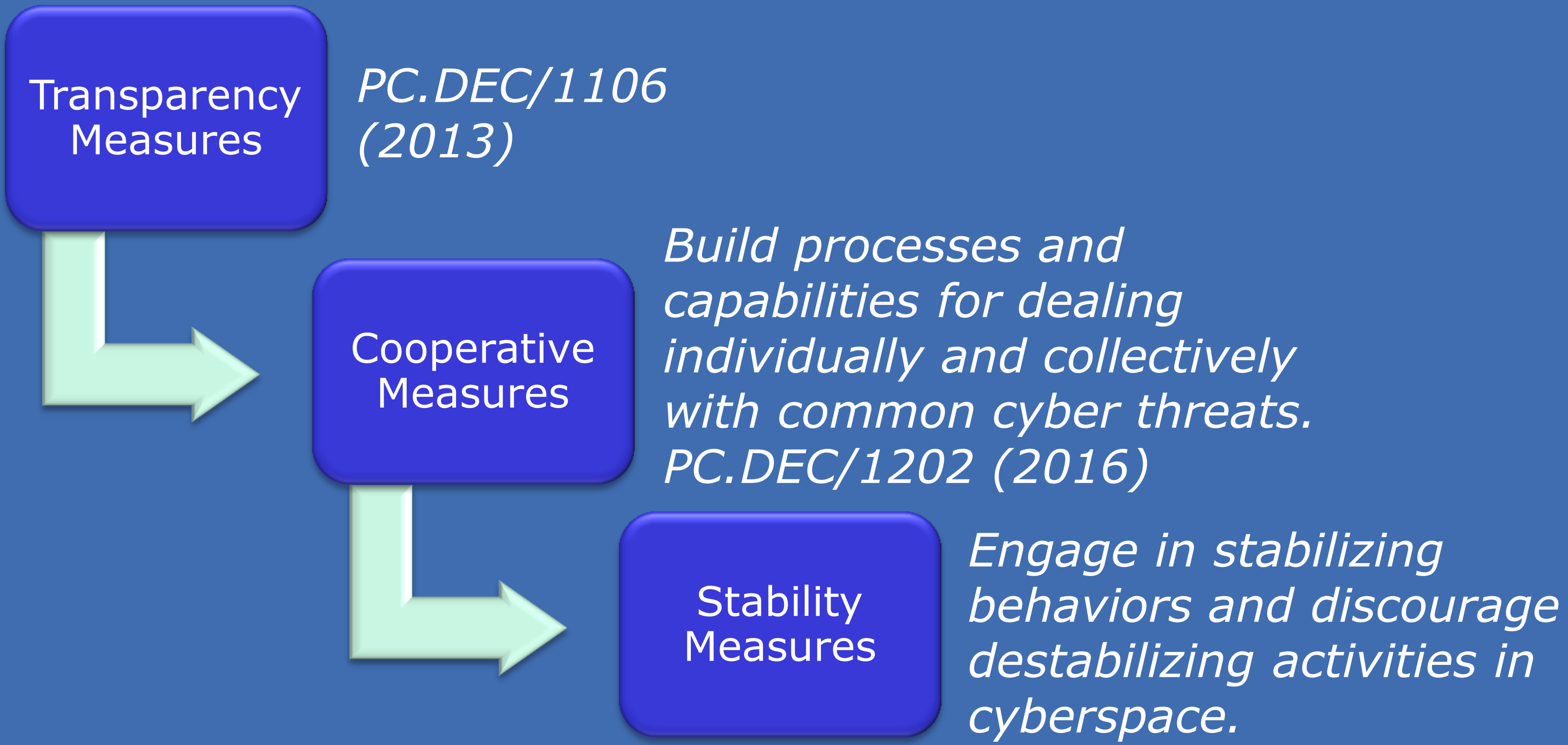
- Measures to increase stability and security in the use of ICTs;
- Responses to ICT incidents;
- The use of State’s territory for internationally wrongful acts;
- Cooperation concerning terrorist and criminal use of ICTs;
- Respect for human rights;
- ICT activity that intentionally damages critical infrastructure;
- States’ measures to protect their critical infrastructure from ICT threats;
- Responses to requests for assistance in mitigating malicious ICT acts;
- The integrity of the supply chain, so that end users can have confidence in the security of ICT products;
- Reporting of ICT vulnerabilities and information on available remedies; and
- The role of CERTs.

Regional organizations bring together those states that are most likely to have tense relations. Regional organizations provide a forum for such neighbors to talk, and, ideally, to resolve their grievances. This is especially valuable regarding cyber-conflict.



None
Private Individual
No
Domestic Political Group
Deliberate?
Intstigated by…
Political Significance
Cyber Incident
Foreign Political Group
Deliberate?
Yes
Instigated by…
Foreign State
High

OSCE Three-Step Approach to Cyber Confidence Building



Transparency Measures

PC.DEC/1106 (2013)

Cooperative Measures

Build processes and capabilities for dealing individually and collectively with common cyber threats. PC.DEC/1202 (2016)

Stability Measures

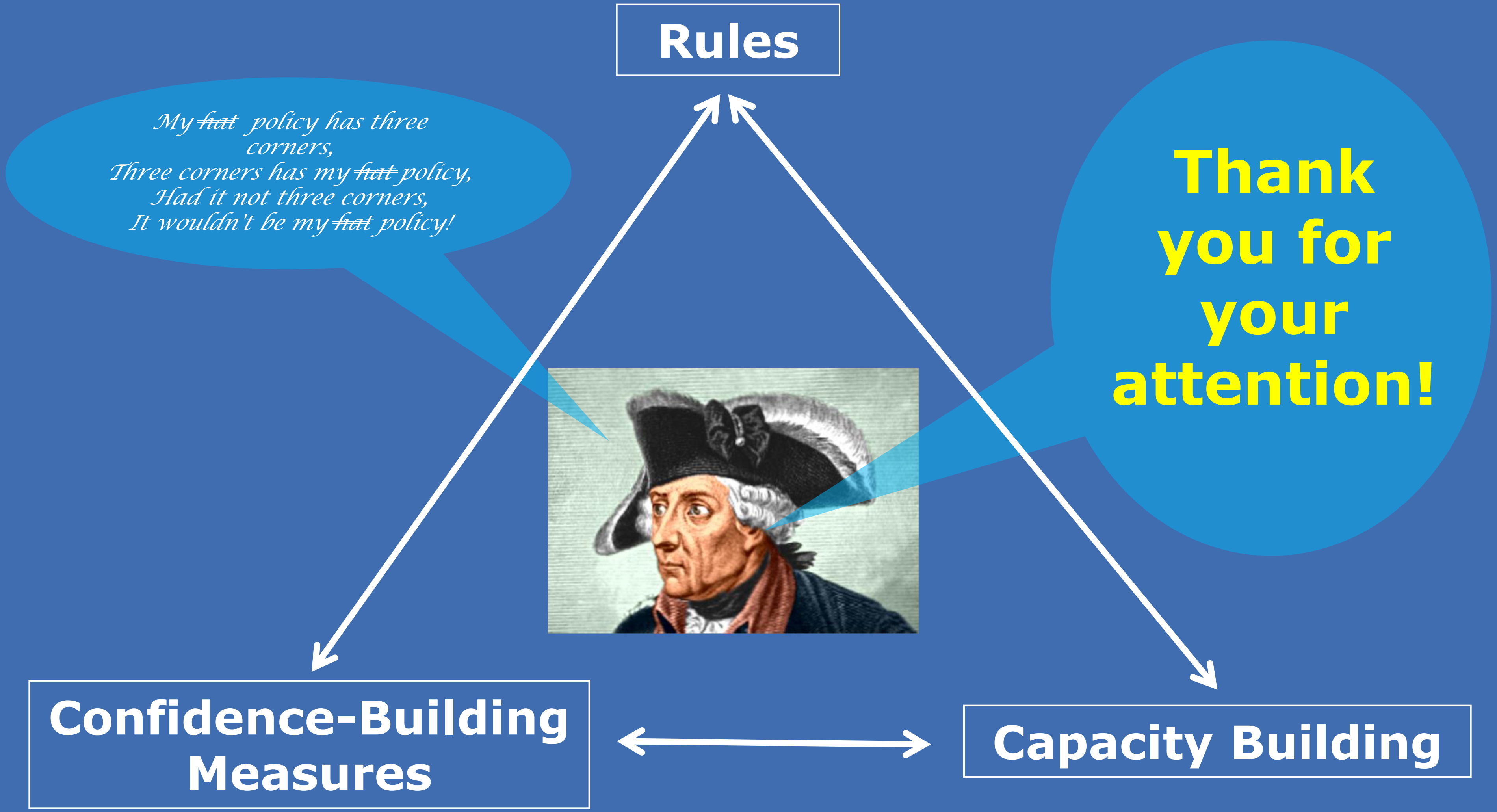
Engage in stabilizing behaviors and discourage destabilizing activities in cyberspace.

"Cyber 3 D":

Multiple Dimensions of Cyber Security

Cyber Security Capacity Building can enable others to adhere to the rules of responsible state behavior. However, we are seeing relatively sparse action by digital advanced countries.

We need bilateral and multilateral cooperation initiatives that would build on established partnership relations.



Rules

My ~~hat~~ policy has three corners,
Three corners has my ~~hat~~ policy,
Had it not three corners,
It wouldn't be my ~~hat~~ policy!

Thank you for your attention!

Confidence-Building Measures

Capacity Building