CSBMs for Cyber Forces?

Jürgen Altmann
TU Dortmund University
Dortmund, Germany

OSCE Security Chat

The Framework for Arms Control in an Age of Emerging Technologies

Webinar

16 June 2021

Based on
Jürgen Altmann, Gian Piero Siroli, Confidence and Security Building Measures for the Cyber Realm, 2018, in: A. Masys (ed.), Handbook of Security Science, Cham: Springer, https://doi.org/10.1007/978-3-319-51761-2_59-1
See also:
Jürgen Altmann, Confidence and Security Building Measures for Cyber Forces, in C. Reuter (ed.), Information Technology for Peace and Security – IT Applications and Infrastructures in Conflicts, Crises, War and Peace, Wiesbaden: Springer Vieweg, 2019

Cyber Forces: threats to international security and military stability

Dozens of states have built up cyber forces

They work in relative secrecy and have not only defensive, but also offensive purposes

They prepare for effects not only in the cyber sphere, but also in the physical world, against military forces as well as civilian infrastructure

There is the threat of retaliation in the physical world.

With the need for very fast reaction comes destabilisation, in particular if cyber systems use automatic reaction. This creates dangers for international security.

Arms control dearly needed, but difficult
Cyber weapons less tangible than battle tanks and combat aircraft
Need more secrecy

Concepts for cyber arms control and verification require creativity and research – some ideas exist,* but much more work is needed

As long as arms control seems difficult: look at Confidence and Security Building measures as a start
"Security" meaning: for armed forces

* Reinhold/Reuter, Chs. 10, 12 in Reuter 2019 (see p. 1)

Agreed Cyber CBMs (without “S”) acknowledge these dangers

UN GGE 2017:

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

States are rightfully concerned about the danger of destabilizing misperceptions, the potential for conflict and the possibility of harm to their citizens, property and economy”

OSCE 2016:

“to enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs”

But: they are voluntary and non-binding

And do not cover military forces

There are CSBMs for land/air forces in Europe Defined in the Vienna Document 2011 of the OSCE

60 pages, very detailed

E.g. in Chapter 1, information exchange:

ANNEX III

(1)	BATTLE TANKS	
(1.1)	Type	
(1.2)	National Nomenclature/Name	
(1.3)	Main Gun Calibre	
(1.4)	Unladen Weight	
(1.5)	Data on new types or versions will, in addition, include:	
(1.5.1)	Night Vision Capability	yes/no
(1.5.2)	Additional Armour	yes/no
(1.5.3)	Track Width	cm
(1.5.4)	Floating Capabilities	yes/no
(1.5.5)	Snorkelling Equipment	yes/no

+ photographs presenting the right or left side, top and front views

They are obligatory and politically binding

Could some of them be transferred to cyber forces?

Chapters of the Vienna Document 2011

I. Exchange of military information - forces: **Organization, manpower** **Major weapon/equipment systems** **Plans for deployment**
II. Exchange of information **Policy/doctrines, force planning, budgets/expenditures, clarification/review/dialogue**
III. Risk reduction **Consultation and co-operation about unusual/hazardous activities** **Voluntary hosting of visits to dispel concerns**
IV. Contacts **Visits, military contacts/cooperation, demonstration new weapon/equipment types**
V. Prior notification of certain military activities above thresnolds
VI. Observation of certain military activities above thresnolds
VII. Annual calendars of military activities above thresholds
VIII. Constraining provisions – Large activities
IX. Compliance, verification – National technical means **Inspections ground/air, Evaluation visits**
X. Regional measures
XI. Annual implementation assessment meeting
Conflict Prevention Centre

Transfer to Cyber Forces? Some easy, others very difficult

I. Exchange of military information - Cyber forces: Organization, manpower Cyber weapons Plans for deployment	+ Very intrusive Difficult to define/implement
II. Exchange of information Cyber-defense policy/doctrines, force planning, budgets/expenditures, clarification/review/dialogue	Already partly in OSCE CBM 7
III. Risk reduction Consultation and co-operation about unusual/hazardous activities Voluntary hosting of visits to dispel concerns	In part already in OSCE CBMs +
IV. Contacts Visits to bases, military contacts/cooperation, demonstration new weapon/equipment types	Very intrusive
V. Prior notification of certain military cyber activities	Very intrusive, difficult to define/ implement
VI. Observation of certain military cyber activities	Very intrusive
VII. Annual calendars of military cyber activities	Difficult to define/implement
VIII. Constraining provisions – Large activities	Difficult to define/implement
IX. Compliance, verification – National technical means Inspections, Evaluation visits	+ Very intrusive
X. Regional measures	In part already in OSCE CBMs
XI. Annual implementation assessment meeting	In part already in OSCE CBMs
Conflict Prevention Centre	+

Conclusion

Some of the OSCE CSBMs could be transferred to cyber forces relatively easily; some are even possible under the existing voluntary OSCE cyber CBMs

Some would be difficult to define and implement

Some would be very intrusive and probably not acceptable under present circumstances

States should take CSBMs for cyber forces into consideration and discuss which ones could be agreed upon – implemented e.g. by extending the Vienna Document